Procedimientos de administradores de Trusted Extensions

Referencia: E38865–10
Enero de 2013



130224@25097

Contenido

Lista de figuras

Lista de tablas

Prefacio

La guía *Procedimientos de administradores de Trusted Extensions* proporciona los procedimientos para configurar Trusted Extensions en el Sistema operativo Oracle Solaris (SO Oracle Solaris). Además, esta guía brinda información acerca de los procedimientos para gestionar usuarios, zonas, dispositivos y hosts con etiquetas del software de Trusted Extensions.

Nota – Esta versión de Oracle Solaris es compatible con sistemas que usen arquitecturas de las familias de procesadores SPARC y x86. Los sistemas compatibles aparecen en *Listas de compatibilidad del sistema operativo Oracle Solaris*. Este documento indica las diferencias de implementación entre los tipos de plataforma.

En este documento, estos términos relacionados con x86 significan lo siguiente:

- x86 hace referencia a la familia más grande de productos compatibles con x86 de 32 y 64 bits.
- x64 hace referencia específicamente a CPU compatibles con x86 de 64 bits.
- "x86 de 32 bits" destaca información específica de 32 bits acerca de sistemas basados en x86.

Para conocer cuáles son los sistemas admitidos, consulte *Listas de compatibilidad del sistema operativo Oracle Solaris*.

Usuarios a los que está destinada esta guía

Esta guía está destinada a administradores de sistemas y administradores de seguridad expertos que deben configurar y administrar el software Trusted Extensions. El nivel de confianza que requiere la política de seguridad del sitio y el grado de experiencia necesario determinan quién puede realizar las tareas de configuración.

Los administradores deben estar familiarizados con la administración de Oracle Solaris. Asimismo, los administradores deben comprender lo siguiente:

- Las funciones de seguridad de Trusted Extensions y la política de seguridad del sitio
- Los procedimientos y conceptos básicos para usar un host configurado con Trusted Extensions, según lo descrito en la *Trusted Extensions User's Guide*
- La manera en que se dividen las tareas administrativas entre los roles en el sitio

Cómo se organizan las guías de Trusted Extensions

En la tabla siguiente, se enumeran los temas que se tratan en las guías de Trusted Extensions y los destinatarios de cada guía.

Título de la guía	Temas	Destinatarios
Trusted Extensions User's Guide	Describe las funciones básicas de Trusted Extensions. Este manual contiene un glosario.	Usuarios finales, administradores y desarrolladores
Trusted Extensions Configuration Guide	A partir de la versión Solaris 10 5/08, describe cómo activar y configurar inicialmente Trusted Extensions. Reemplaza a *Solaris Trusted Extensions Installation and Configuration for the Solaris 10 11/06 and Solaris 10 8/07 Releases*.	Administradores y desarrolladores
Procedimientos de administradores de Trusted Extensions	Muestra cómo realizar tareas de administración específicas.	Administradores y desarrolladores
Trusted Extensions Developer's Guide	Describe cómo desarrollar aplicaciones con Trusted Extensions.	Desarrolladores y administradores
Trusted Extensions Label Administration	Proporciona información sobre cómo especificar componentes de etiquetas en el archivo de codificaciones de etiqueta.	Administradores
Compartmented Mode Workstation Labeling: Encodings Format	Describe la sintaxis utilizada en el archivo de codificaciones de etiqueta. La sintaxis aplica distintas reglas para dar un formato correcto a las etiquetas de un sistema.	Administradores

Guías de administración del sistema relacionadas

Las siguientes guías contienen información que resulta útil en el momento de preparar y ejecutar software de Trusted Extensions.

Título del manual	Temas
Administración de Oracle Solaris: administración básica	Grupos y cuentas de usuario, asistencia para clientes y servidores, cierre e inicio de un sistema, administración de servicios y administración de software (paquetes y parches)
Guía de administración del sistema: Administración avanzada	Terminales y módems, recursos del sistema (cuotas de disco, cuentas y archivos crontab), procesos del sistema y resolución de problemas de software de Solaris
System Administration Guide: Devices and File Systems	Medios extraíbles, discos y dispositivos, sistemas de archivos y copias de seguridad y restauración de datos.

Título del manual	Temas
Administración de Oracle Solaris: servicios IP	Administración de redes TCP/IP, administración de direcciones IPv4 e IPv6, DHCP, IPsec, IKE, filtro IP de Solaris, IP para móviles, multirruta IP de Solaris (IPMP) e IPQoS
Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP).	Servicios de directorios y nombres DNS, NIS y LDAP, incluida la transición de NIS a LDAP y de NIS+ a LDAP
Guía de administración del sistema: servicios de red	Servidores de caché Web, servicios relacionados con el tiempo, sistemas de archivos de red (NFS y Autofs), correo, SLP y PPP
System Administration Guide: Security Services	Auditoría, administración de dispositivos, seguridad de archivos, BART, servicios Kerberos, PAM, estructura criptográfica de Solaris, privilegios, RBAC, SASL y Solaris Secure Shell
Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris	Tareas y proyectos de temas de administración de recursos, contabilidad extendida, controles de recursos, planificación por reparto equitativo (FSS), control de memoria física utilizando el daemon de limitación de recursos (rcapd) y agrupaciones de recursos; virtualización con la tecnología de partición de software Zonas de Solaris y zonas con la marca `lx`
Guía de administración de Oracle Solaris ZFS	Creación y gestión de sistemas de archivos y agrupaciones de almacenamiento ZFS, instantáneas, clones, copias de seguridad, uso de listas de control de acceso (ACL) para proteger archivos ZFS, uso de Solaris ZFS en un sistema Solaris con zonas instaladas, volúmenes emulados y solución de problemas y recuperación de datos.
System Administration Guide: Printing	Tareas y temas de impresión de Solaris, el uso de servicios, herramientas, protocolos y tecnologías para configurar y administrar las impresoras y los servicios de impresión

Referencias relacionadas

Documento de la política de seguridad del sitio: describe la política y los procedimientos de seguridad de seguridad del sitio.

Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide: describe el entorno de escritorio común (CDE, Common Desktop Environment)

Guía del administrador para el sistema operativo instalado actualmente: describe cómo realizar una copia de seguridad de los archivos del sistema.

Referencias relacionadas con el sitio web de otras empresas

En este documento, se proporcionan direcciones URL de terceros e información adicional relacionada.

Nota – Oracle no se hace responsable de la disponibilidad de los sitios web de terceros que se mencionen en este documento. Oracle no garantiza ni se hace responsable de los contenidos, la publicidad, los productos u otros materiales que puedan estar disponibles en dichos sitios o recursos, o a través de dichos sitios o recursos. Oracle no se responsabiliza de ningún daño, real o supuesto, ni de posibles pérdidas que se pudieran derivar del uso de los contenidos, bienes o servicios que estén disponibles en dichos sitios o recursos.

Acceso a Oracle Support

Los clientes de Oracle tienen acceso a soporte electrónico por medio de My Oracle Support. Para obtener más información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o, si tiene alguna discapacidad auditiva, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`.

Convenciones tipográficas

La siguiente tabla describe las convenciones tipográficas utilizadas en este manual.

TABLA P–1 Convenciones tipográficas

Tipos de letra	Descripción	Ejemplo
`AaBbCc123`	Los nombres de los comandos, los archivos, los directorios y los resultados que el equipo muestra en pantalla	Edite el archivo `.login`. Utilice el comando `ls -a` para mostrar todos los archivos. `nombre_sistema% tiene correo.`
`AaBbCc123`	Lo que se escribe, en contraposición con la salida del equipo en pantalla	`nombre_sistema%` **`su`** `Contraseña:`
aabbcc123	Marcador de posición: sustituir por un valor o nombre real	El comando necesario para eliminar un archivo es `rm` *filename*.

TABLA P–1 Convenciones tipográficas *(Continuación)*

Tipos de letra	Descripción	Ejemplo
AaBbCc123	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el capítulo 6 de la *Guía del usuario*. Una *copia en caché* es aquella que se almacena localmente. *No* guarde el archivo. **Nota:** Algunos elementos destacados aparecen en negrita en línea.

Indicadores de los shells en los ejemplos de comandos

La tabla siguiente muestra los indicadores de sistema UNIX y los indicadores de superusuario para shells incluidos en el sistema operativo Oracle Solaris. En los ejemplos de comandos, el indicador de shell muestra si el comando debe ser ejecutado por un usuario normal o un usuario con privilegios.

TABLA P–2 Indicadores de shell

Shell	Indicador
Shell Bash, shell Korn y shell Bourne	`$`
Shell Bash, shell Korn y shell Bourne para superusuario	`#`
Shell C	`machine_name%`
Shell C para superusuario	`machine_name#`



CAPÍTULO 1

Conceptos de la administración de Trusted Extensions

En este capítulo, se presenta la administración de un sistema que está configurado con el software de Trusted Extensions.

- "Software de Trusted Extensions y el SO Oracle Solaris" en la página 23
- "Conceptos básicos de Trusted Extensions" en la página 26

Software de Trusted Extensions y el SO Oracle Solaris

El software de Trusted Extensions agrega etiquetas a un sistema que ejecuta el sistema operativo Solaris (SO Oracle Solaris). Las etiquetas implementan el *control de acceso obligatorio* (MAC, Mandatory Access Control). El MAC, junto con el control de acceso discrecional (DAC, Discretionary Access Control), protege los sujetos (procesos) y objetos (datos) del sistema. El software Trusted Extensions proporciona interfaces para gestionar la configuración, la asignación y la política de etiquetas.

Similitudes entre Trusted Extensions y el SO Oracle Solaris

El software de Trusted Extensions utiliza perfiles de derechos, roles, auditoría, privilegios y otras funciones de seguridad del SO Oracle Solaris. Puede utilizar Oracle Solaris Secure Shell (SSH), BART, la estructura criptográfica de Oracle Solaris, IPsec o Filtro IP con Trusted Extensions.

- Como en el SO Oracle Solaris, los usuarios pueden estar limitados a utilizar las aplicaciones que son necesarias para realizar su trabajo. Se puede autorizar a otros usuarios para que realicen más tareas.
- Como en el SO Oracle Solaris, las capacidades que antes estaban asignadas al superusuario se asignan a "roles" individuales y discretos.

- Como en el SO Oracle Solaris, los privilegios protegen los procesos. También se utilizan las zonas para procesos independientes.
- Como en el SO Oracle Solaris, se pueden auditar los eventos del sistema.
- Trusted Extensions utiliza los archivos de configuración del sistema del SO Oracle Solaris, como `policy.conf` y `exec_attr`.

Diferencias entre Trusted Extensions y el SO Oracle Solaris

El software Trusted Extensions amplía el SO Oracle Solaris. La siguiente lista proporciona una descripción general. Para obtener una referencia rápida, consulte el Apéndice A, "Referencia rápida a la administración de Trusted Extensions".

- Trusted Extensions controla el acceso a los datos mediante marcas de seguridad especiales que se denominan *etiquetas*. Las etiquetas proporcionan el *control de acceso obligatorio* (MAC). Se brinda la protección de MAC además de los permisos de archivos UNIX o el control de acceso discrecional (DAC). Las etiquetas se asignan directamente a los usuarios, las zonas, los dispositivos, las ventanas y los puntos finales de red. De manera implícita, las etiquetas se asignan a los procesos, los archivos y otros objetos del sistema.

  Los usuarios comunes no pueden invalidar el MAC. Trusted Extensions requiere que los usuarios comunes operen en las zonas con etiquetas. De manera predeterminada, ningún usuario o proceso de las zonas con etiquetas puede invalidar el MAC.

  Como en el SO Oracle Solaris, la capacidad de invalidar la política de seguridad puede asignarse a procesos o usuarios específicos en los casos en que puede invalidarse el MAC. Por ejemplo, los usuarios pueden estar autorizados para cambiar la etiqueta de un archivo. Este tipo de acciones aumentan o disminuyen el nivel de sensibilidad de la información en dicho archivo.
- Trusted Extensions complementa los comandos y los archivos de configuración existentes. Por ejemplo, Trusted Extensions agrega eventos de auditoría, autorizaciones, privilegios y perfiles de derechos.
- Algunas funciones que son opcionales en un sistema Oracle Solaris son obligatorias en un sistema Trusted Extensions. Por ejemplo, las zonas y los roles son necesarios en un sistema que esté configurado con Trusted Extensions.
- Algunas funciones que son opcionales en un sistema Oracle Solaris son recomendadas en un sistema Trusted Extensions. Por ejemplo, en Trusted Extensions, el usuario `root` debe transformarse en el rol `root`.
- Trusted Extensions puede cambiar el comportamiento predeterminado del SO Oracle Solaris. Por ejemplo, en un sistema configurado con Trusted Extensions, la auditoría está activada de manera predeterminada. También se requiere la asignación de dispositivos.

- Trusted Extensions puede reducir la oferta de opciones que están disponibles en el SO Oracle Solaris. Por ejemplo, en un sistema que está configurado con Trusted Extensions, no se admite el servicio de nombres NIS+. Además, en Trusted Extensions, todas las zonas son zonas con etiquetas. A diferencia del SO Oracle Solaris, las zonas con etiquetas deben utilizar la misma agrupación de ID de usuario e ID de grupo. Asimismo, en Trusted Extensions, las zonas con etiquetas pueden compartir una dirección IP.
- Trusted Extensions proporciona versiones de confianza de dos escritorios. Para trabajar en un entorno con etiquetas, los usuarios de escritorios de Trusted Extensions deben utilizar uno de los siguientes escritorios:
  - **Solaris Trusted Extensions (CDE)**: es la versión de confianza del entorno de escritorio común (CDE, Common Desktop Environment). Puede abreviarse como Trusted CDE.
  - **Solaris Trusted Extensions (JDS)**: es la versión de confianza de Java Desktop System, versión *number*. Puede abreviarse como Trusted JDS.
- Trusted Extensions proporciona interfaces gráficas de usuario (GUI) e interfaces de la línea de comandos (CLI) adicionales. Por ejemplo, Trusted Extensions proporciona Device Allocation Manager para administrar dispositivos. Además, el comando `updatehome` se utiliza para colocar los archivos de inicio en el directorio principal de un usuario común en cada etiqueta.
- Trusted Extensions requiere el uso de determinadas interfaces gráficas de usuario para la administración. Por ejemplo, en un sistema que está configurado con Trusted Extensions, se utiliza la consola Solaris Management Console para administrar los usuarios, los roles y la red. Asimismo, en Trusted CDE, Admin Editor se utiliza para editar los archivos del sistema.
- Trusted Extensions limita lo que pueden visualizar los usuarios. Por ejemplo, el usuario que no puede asignar un dispositivo tampoco puede visualizarlo.
- Trusted Extensions limita las opciones de escritorio de los usuarios. Por ejemplo, los usuarios disponen de un tiempo limitado de inactividad de la estación de trabajo antes de que se bloquee la pantalla.

Sistemas de varios periféricos y escritorio de Trusted Extensions

Cuando los monitores de un sistema de varios periféricos de Trusted Extensions están configurados de forma horizontal, la banda de confianza abarca todos los monitores. Cuando los monitores están configurados de forma vertical, la banda de confianza aparece en el monitor ubicado en el extremo inferior.

Cuando los distintos espacios de trabajo se muestran en los supervisores de un sistema de varios encabezados, Trusted CDE y Trusted JDS procesan la banda de confianza de diferentes maneras.

- En el escritorio de Trusted JDS, cada supervisor muestra una banda de confianza.

- En el escritorio de Trusted CDE, aparece una banda de confianza en el supervisor principal.



Precaución – Si aparece una segunda banda de confianza en un sistema de varios encabezados de Trusted CDE, el sistema operativo no genera la banda. Es posible que tenga un programa no autorizado en el sistema.

Póngase en contacto con el administrador de la seguridad inmediatamente. Para determinar qué banda de confianza es la adecuada, consulte "Cómo recuperar el control del enfoque actual del escritorio" en la página 72.

Conceptos básicos de Trusted Extensions

El software Trusted Extensions agrega etiquetas a un sistema Oracle Solaris. También se agregan los escritorios con etiquetas y las aplicaciones de confianza, como Label Builder y Device Allocation Manager. Los conceptos de esta sección son necesarios para que los usuarios y los administradores comprendan Trusted Extensions. En la *Trusted Extensions User's Guide*, se presentan estos conceptos para los usuarios.

Protecciones de Trusted Extensions

El software de Trusted Extensions mejora la protección del SO Oracle Solaris. El SO Oracle Solaris protege el acceso al sistema mediante cuentas de usuario que requieren contraseñas. Se puede requerir que las contraseñas deban cambiarse con regularidad, que tengan una extensión determinada, etcétera. Los roles requieren contraseñas adicionales para realizar tareas administrativas. La autenticación adicional limita el daño que puede ocasionar un intruso que adivina la contraseña del usuario root, ya que los roles no pueden utilizarse como cuentas de entrada. El software de Trusted Extensions mejora aún más este aspecto al restringir a los usuarios y los roles a un rango de etiquetas aprobado. Este rango de etiquetas limita la información a la que pueden acceder los usuarios y los roles.

El software Trusted Extensions muestra el símbolo de Trusted Path, un emblema inconfundible y a prueba de falsificaciones que aparece a la izquierda de la banda de confianza. En Trusted CDE, la banda se encuentra en la parte inferior de la pantalla. En Trusted JDS, la banda se muestra en la parte superior de la pantalla. El símbolo de Trusted Path les indica a los usuarios que están utilizando partes del sistema relacionadas con la seguridad. Si este símbolo no aparece cuando el usuario está ejecutando una aplicación de confianza, debe comprobarse inmediatamente la autenticidad de esa versión de la aplicación. Si la banda de confianza no aparece, el escritorio no es de confianza. Para ver un ejemplo de la visualización del escritorio, consulte la Figura 1–1.

FIGURA 1–1 Escritorio de CDE de varios niveles en Trusted Extensions

Menú Trusted Path
Banda de etiqueta de ventana
Banda de etiqueta de ícono de ventana
Panel frontal
Banda de confianza
Símbolo de confianza
Etiqueta de espacio de trabajo

La mayor parte del software relacionado con la seguridad, es decir, la base de computación de confianza (TCB, Trusted Computing Base), se ejecuta en la zona global. Los usuarios comunes no pueden entrar en la zona global ni visualizar sus recursos. Los usuarios pueden interactuar con el software de TCB, como cuando modifican las contraseñas. El símbolo de Trusted Path se muestra cuando el usuario interactúa con la TCB.

Trusted Extensions y el control de acceso

El software Trusted Extensions protege la información y otros recursos mediante el control de acceso discrecional (DAC) y el control de acceso obligatorio (MAC). El DAC corresponde a las listas de control de acceso y los bits de permiso tradicionales de UNIX que están configurados según el criterio del propietario. El MAC es un mecanismo que el sistema pone en funcionamiento automáticamente. El MAC controla todas las transacciones mediante la comprobación de las etiquetas de los procesos y los datos de la transacción.

La *etiqueta* del usuario representa el nivel de sensibilidad en que el usuario tiene permitido operar y que, a la vez, elige para operar. Las etiquetas típicas son `Secret` o `Public`. La etiqueta determina la información a la que puede acceder el usuario. Es posible invalidar el MAC y el

DAC mediante permisos especiales que están en el SO Oracle Solaris. Los *privilegios* son permisos especiales que pueden otorgarse a los procesos. Las *autorizaciones* son permisos especiales que puede otorgar el administrador a los usuarios y los roles.

Como administrador, debe brindar a los usuarios formación sobre los procedimientos adecuados para proteger los archivos y los directorios, en función de la política de seguridad del sitio. Además, debe indicar a los usuarios que estén autorizados a subir o bajar el nivel de las etiquetas cuál es el momento adecuado para hacerlo.

Roles y Trusted Extensions

En un sistema que ejecuta el software Oracle Solaris sin Trusted Extensions, los roles son opcionales. En un sistema que está configurado con Trusted Extensions, los roles son necesarios. Los roles de administrador del sistema y de administrador de la seguridad administran el sistema. En algunos casos, se utiliza el rol `root`.

Como en el SO Oracle Solaris, los perfiles de derechos son la base de las capacidades de un rol. Trusted Extensions proporciona dos perfiles de derechos: el de seguridad de la información y el de seguridad del usuario. Estos dos perfiles definen el rol de administrador de la seguridad.

Los programas que están disponibles para un rol en Trusted Extensions tienen una propiedad especial: el *atributo de la ruta de confianza*. Este atributo indica que el programa es parte de la TCB. El atributo de la ruta de confianza está disponible cuando un programa se inicia desde la zona global.

Para obtener información sobre los roles, consulte la Parte III, "Roles, Rights Profiles, and Privileges" de *System Administration Guide: Security Services*.

Etiquetas en el software Trusted Extensions

Las etiquetas y las acreditaciones son fundamentales para el control de acceso obligatorio (MAC) en Trusted Extensions. Determinan qué usuarios pueden acceder a qué programas, archivos y directorios. Las etiquetas y las acreditaciones contienen un componente de *clasificación* y, además, puede que no contengan ningún componente de *compartimiento* o que contengan algunos. El componente de clasificación señala el nivel jerárquico de seguridad, como `TOP SECRET` o `CONFIDENTIAL`. El componente de compartimiento representa un grupo de usuarios que podrían necesitar acceso a un cuerpo común de información. Algunos de los ejemplos de tipos de compartimientos más comunes son los proyectos, los departamentos o las ubicaciones físicas. Las etiquetas son legibles para los usuarios autorizados, pero internamente se las manipula como números. En el archivo `label_encodings`, se definen los números y las versiones legibles correspondientes.

Trusted Extensions media en todas las transacciones relacionadas con la seguridad que se hayan intentado realizar. El software compara las etiquetas de la entidad de acceso (por lo general, un proceso) y la entidad a la que se accede (normalmente, un objeto del sistema de archivos).

Luego, el software permite o no realizar la transacción según qué etiqueta sea *dominante*. También se utilizan las etiquetas para determinar el acceso a otros recursos del sistema, como dispositivos asignables, redes, búferes de trama y otros hosts.

Relaciones de dominio entre etiquetas

Se dice que la etiqueta de una entidad *domina* otra etiqueta si se cumplen las dos condiciones siguientes:

- El componente de clasificación de la etiqueta de la primera entidad es mayor o igual que la clasificación de la segunda entidad. El administrador de la seguridad asigna números a las clasificaciones en el archivo `label_encodings`. El software compara estos números para determinar el dominio.
- El conjunto de compartimientos de la primera entidad incluye todos los compartimientos de la segunda entidad.

Se dice que dos etiquetas son *iguales* si tienen la misma clasificación y el mismo conjunto de compartimientos. Si las etiquetas son iguales, se dominan entre sí, y se permite el acceso.

Si una etiqueta tiene una clasificación superior o tiene la misma clasificación y los compartimientos son un superconjunto de los compartimientos de la segunda etiqueta, o si se cumplen ambas condiciones, se dice que la primera etiqueta *domina estrictamente* la segunda etiqueta.

Se dice que dos etiquetas están *separadas* o *no son comparables* si ninguna de ellas domina la otra.

La siguiente tabla presenta algunos ejemplos sobre comparaciones de etiquetas con relación al dominio. En el ejemplo, `NEED_TO_KNOW` es una clasificación superior a `INTERNAL`. Hay tres compartimientos: Eng, Mkt y Fin.

TABLA 1–1 Ejemplos de relaciones de etiquetas

Etiqueta 1	Relación	Etiqueta 2
`NEED_TO_KNOW Eng Mkt`	domina (estrictamente)	`INTERNAL Eng Mkt`
`NEED_TO_KNOW Eng Mkt`	domina (estrictamente)	`NEED_TO_KNOW Eng`
`NEED_TO_KNOW Eng Mkt`	domina (estrictamente)	`INTERNAL Eng`
`NEED_TO_KNOW Eng Mkt`	domina (de igual modo)	`NEED_TO_KNOW Eng Mkt`
`NEED_TO_KNOW Eng Mkt`	está separada de	`NEED_TO_KNOW Eng Fin`
`NEED_TO_KNOW Eng Mkt`	está separada de	`NEED_TO_KNOW Fin`
`NEED_TO_KNOW Eng Mkt`	está separada de	`INTERNAL Eng Mkt Fin`

Etiquetas administrativas

Trusted Extensions proporciona dos etiquetas administrativas especiales que se utilizan como etiquetas o acreditaciones: `ADMIN_HIGH` y `ADMIN_LOW`. Estas etiquetas se utilizan para proteger los recursos del sistema y no están diseñadas para los usuarios comunes, sino para los administradores.

`ADMIN_HIGH` es la etiqueta máxima. `ADMIN_HIGH` domina el resto de las etiquetas del sistema y se utiliza para evitar la lectura de los datos del sistema, como las bases de datos de administración o las pistas de auditoría. Debe estar en la zona global para leer los datos con la etiqueta `ADMIN_HIGH`.

`ADMIN_LOW` es la etiqueta mínima. `ADMIN_LOW` está dominada por el resto de las etiquetas de un sistema, incluidas las etiquetas de los usuarios comunes. El control de acceso obligatorio no permite que los usuarios escriban datos en los archivos con etiquetas de un nivel inferior al de la etiqueta del usuario. Por lo tanto, los usuarios comunes pueden leer un archivo con la etiqueta `ADMIN_LOW`, pero no pueden modificarlo. `ADMIN_LOW` se utiliza normalmente para proteger los archivos ejecutables que son públicos y están compartidos, como los archivos de `/usr/bin`.

Archivo de codificaciones de etiqueta

Todos los componentes de etiqueta de un sistema, es decir, las clasificaciones, los compartimientos y las reglas asociadas, se almacenan en un archivo `ADMIN_HIGH`: el archivo `label_encodings`. Este archivo se encuentra en el directorio `/etc/security/tsol`. El administrador de la seguridad configura el archivo `label_encodings` para el sitio. Un archivo de codificaciones de etiqueta contiene lo siguiente:

- **Definiciones de componente**: son las definiciones de clasificaciones, compartimientos, etiquetas y acreditaciones, incluidas las reglas para las restricciones y las combinaciones necesarias
- **Definiciones de rangos de acreditación**: es la especificación de las acreditaciones y las etiquetas mínimas que definen los conjuntos de etiquetas disponibles para todo el sistema y los usuarios comunes
- **Especificaciones de impresión**: representan la identificación y el tratamiento de la información para imprimir la página de la carátula, las páginas del ubicador, el encabezado, el pie de página y otras funciones de seguridad en el resultado de la impresión
- **Personalizaciones**: son las definiciones locales que incluyen los códigos de color de etiquetas y otros valores predeterminados

Para obtener más información, consulte la página del comando man `label_encodings(4)`. También se puede encontrar información detallada en *Trusted Extensions Label Administration* y *Compartmented Mode Workstation Labeling: Encodings Format* .

Rangos de etiquetas

Un *rango de etiquetas* es el conjunto de etiquetas potencialmente utilizables en que pueden operar los usuarios. Tanto los usuarios como los recursos tienen rangos de etiquetas. Los rangos de etiquetas pueden proteger recursos que incluyen elementos como dispositivos asignables, redes, interfaces, búferes de trama y comandos o acciones. Un rango de etiquetas está definido por una acreditación en la parte superior del rango y una etiqueta mínima en la parte inferior.

Un rango no incluye necesariamente todas las combinaciones de etiquetas que se ubican entre una etiqueta máxima y una etiqueta mínima. Las reglas del archivo `label_encodings` pueden descartar determinadas combinaciones. Una etiqueta debe estar *bien formada*, es decir, deben permitirla todas las reglas aplicables del archivo de codificaciones de etiqueta a fin de que pueda incluirse en un rango.

No obstante, no es necesario que una acreditación esté bien formada. Imagine, por ejemplo, que un archivo `label_encodings` prohíbe todas las combinaciones de los compartimientos `Eng`, `Mkt` y `Fin` de una etiqueta. `INTERNAL Eng Mkt Fin` sería una acreditación válida, pero no una etiqueta válida. Como acreditación, esta combinación permitiría al usuario acceder a los archivos con las etiquetas `INTERNAL Eng`, `INTERNAL Mkt` e `INTERNAL Fin`.

Rango de etiquetas de cuenta

Cuando se asigna una acreditación y una etiqueta mínima a un usuario, se definen los límites superiores e inferiores del *rango de etiquetas de cuenta* en que puede operar el usuario. La siguiente ecuación describe el rango de etiquetas de cuenta, utilizando ≤ para indicar “dominada por o igual a”:

etiqueta mínima ≤ etiqueta permitida ≤ acreditación

De este modo, el usuario puede operar en cualquier etiqueta que la acreditación domine, siempre que esa etiqueta domine la etiqueta mínima. Cuando no se define expresamente la acreditación o la etiqueta mínima del usuario, se aplican los valores predeterminados que están definidos en el archivo `label_encodings`.

Se pueden asignar una acreditación y una etiqueta mínima a los usuarios que los activen a operar en más de una etiqueta o en una sola etiqueta. Cuando la acreditación y la etiqueta mínima del usuario son iguales, el usuario sólo puede operar en una etiqueta.

Rango de sesión

El *rango de sesión* es el conjunto de etiquetas que están disponibles para un usuario durante una sesión de Trusted Extensions. El rango de sesión deberá estar dentro del rango de etiquetas de cuenta del usuario y el conjunto de rangos de etiquetas del sistema. En el inicio de sesión, si el usuario selecciona el modo de sesión de una sola etiqueta, el rango de sesión se limita a esa etiqueta. Si el usuario selecciona el modo de sesión de varias etiquetas, la etiqueta que el usuario selecciona se convierte en la acreditación de sesión. La acreditación de sesión define el límite

superior del rango de sesión. La etiqueta mínima del usuario define el límite inferior. El usuario inicia la sesión en un espacio de trabajo ubicado en la etiqueta mínima. Durante la sesión, el usuario puede cambiar a un espacio de trabajo que se encuentre en cualquier etiqueta dentro del rango de sesión.

Qué protegen las etiquetas y dónde aparecen

Las etiquetas aparecen en el escritorio y en el resultado que se ejecuta en el escritorio, como el resultado de la impresión.

- **Aplicaciones**: son las aplicaciones que inician los procesos. Dichos procesos se ejecutan en la etiqueta del espacio de trabajo en que se inicia la aplicación. Una aplicación de una zona con etiquetas, como un archivo, se etiqueta en la etiqueta de la zona.
- **Dispositivos**: la asignación de dispositivos y los rangos de etiquetas de dispositivos se utilizan para controlar los datos que se transfieren entre dispositivos. Para utilizar un dispositivo, los usuarios deben ubicarse dentro del rango de etiquetas del dispositivo y estar autorizados para asignar el dispositivo.
- **Puntos de montaje del sistema de archivos**: cada punto de montaje tiene una etiqueta. Se puede visualizar la etiqueta con el comando `getlabel`.
- **Interfaces de red**: las direcciones IP (hosts) tienen plantillas que describen los rangos de etiquetas correspondientes. Los hosts sin etiquetas también tienen una etiqueta predeterminada.
- **Impresoras e impresión**: las impresoras tienen rangos de etiquetas. Las etiquetas se imprimen en las páginas del cuerpo. Las etiquetas, el tratamiento de la información y otros datos de seguridad se imprimen en las páginas de la carátula y del ubicador. Para configurar la impresión en Trusted Extensions, consulte el Capítulo 15, "Gestión de impresión con etiquetas (tareas)" y "Labels on Printed Output" de *Trusted Extensions Label Administration*.
- **Procesos**: los procesos tienen etiquetas. Los procesos se ejecutan en la etiqueta del espacio de trabajo en que se origina cada proceso. Se puede visualizar la etiqueta de un proceso con el comando `plabel`.
- **Usuarios**: se les asignan una etiqueta predeterminada y un rango de etiquetas. La etiqueta del espacio de trabajo del usuario señala la etiqueta de los procesos del usuario.
- **Ventanas**: se pueden visualizar las etiquetas en la parte superior de las ventanas del escritorio. La etiqueta del escritorio también se señala por color. El color aparece en el conmutador del escritorio y encima de las barras de título de las ventanas.

  Cuando se mueve una ventana a un escritorio de trabajo con etiquetas diferentes, la ventana conserva la etiqueta original.
- **Zonas**: cada zona tiene una sola etiqueta. Los archivos y los directorios que son propiedad de una zona se encuentran en la etiqueta de la zona. Para obtener más información, consulte la página del comando man `getzonepath(1)`.



Herramientas de administración de Trusted Extensions

En este capítulo, se describen las herramientas que están disponibles en Trusted Extensions, la ubicación de dichas herramientas y las bases de datos en las que operan.

Herramientas de administración para Trusted Extensions

La administración en los sistemas configurados con Trusted Extensions emplea muchas de las herramientas que se encuentran disponibles en el SO Oracle Solaris. Asimismo, Trusted Extensions ofrece herramientas con mejoras en la seguridad. Los roles pueden acceder a las herramientas de administración únicamente en un espacio de trabajo de rol.

En un espacio de trabajo de rol, puede acceder a los comandos, las acciones, las aplicaciones y las secuencias de comandos que son de confianza. La siguiente tabla proporciona un resumen de estas herramientas administrativas.

TABLA 2–1 Herramientas administrativas de Trusted Extensions

Herramienta	Descripción	Para obtener más información
/usr/sbin/txzonemgr	Proporciona un asistente basado en menú para crear, instalar, inicializar e iniciar las zonas. Esta secuencia de comandos sustituye las acciones de Trusted CDE que administran las zonas. La secuencia de comandos también proporciona opciones de menú para redes y nombres de servicios, y establece la zona global como cliente de un servidor LDAP existente. txzonemgr utiliza el comando zenity.	Consulte "Creating Labeled Zones" de *Trusted Extensions Configuration Guide* También, consulte la página del comando man zenity(1).
En Trusted CDE, acciones en la carpeta Trusted_Extensions en la carpeta Application Manager	Se utiliza para editar archivos locales que Solaris Management Console no gestiona, como /etc/system. Algunas acciones ejecutan secuencias de comandos, como la acción Install Zone.	Consulte "Acciones de Trusted CDE" en la página 35 y "Cómo iniciar acciones administrativas de CDE en Trusted Extensions" en la página 56.
En Trusted CDE, Device Allocation Manager En Solaris Trusted Extensions (JDS), Device Manager	Se utiliza para administrar los rangos de etiquetas de los dispositivos y para asignar o desasignar dispositivos.	Consulte "Device Allocation Manager" en la página 37 y "Control de dispositivos en Trusted Extensions (mapa de tareas)" en la página 245.
Solaris Management Console	Se utiliza para configurar los usuarios, los roles, los derechos, los hosts, las zonas y las redes. Con esta herramienta, pueden actualizarse los archivos locales o las bases de datos LDAP. Con esta herramienta, también puede iniciarse la aplicación heredada dtappsession.	Para conocer acerca de la funcionalidad básica, consulte el Capítulo 2, "Trabajo con Solaris Management Console (tareas)" de *Administración de Oracle Solaris: administración básica*. Para obtener información específica de Trusted Extensions, consulte "Herramientas de Solaris Management Console" en la página 38.
Comandos de Solaris Management Console, como smuser y smtnzonecfg	Es la interfaz de la línea de comandos para Solaris Management Console.	Para ver una lista, consulte la Tabla 2–4.
Generador de etiquetas	Es otra herramienta de usuario. Aparece cuando un programa le solicita que seleccione una etiqueta.	Para obtener un ejemplo, consulte "Cómo modificar el rango de etiquetas de un usuario en Solaris Management Console" en la página 94.
Comandos de Trusted Extensions	Se usan para realizar tareas que no se puedan realizar con las herramientas de Solaris Management Console o las acciones de CDE.	Para ver la lista de comandos administrativos, consulte la Tabla 2–5.

Secuencia de comandos txzonemgr

A partir de la versión Solaris 10 5/08, la secuencia de comandos txzonemgr se utiliza para configurar las zonas con etiquetas. Esta secuencia de comandos zenity(1) muestra un cuadro de diálogo con el título Labeled Zone Manager. Esta GUI presenta un menú con determinación dinámica que muestra únicamente las opciones válidas para el estado de configuración actual de una zona con etiquetas. Por ejemplo, si una zona ya tiene etiquetas, la opción de menú Label no aparece.

Acciones de Trusted CDE

En las tablas siguientes, se enumeran las acciones de CDE que los roles pueden ejecutar en Trusted Extensions. Estas acciones de Trusted CDE se encuentran disponibles en la carpeta Trusted_Extensions. La carpeta Trusted_Extensions se encuentra disponible en la carpeta Application Manager, en el escritorio de CDE.

TABLA 2–2 Acciones administrativas en Trusted CDE, su finalidad y los perfiles de derechos asociados

Nombre de la acción	Finalidad de la acción	Perfil de derechos predeterminado
Add Allocatable Device	Crear dispositivos mediante la agregación de entradas en las bases de datos de los dispositivos. Consulte add_allocatable(1M).	Device Security
Admin Editor	Editar un archivo especificado. Consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.	Object Access Management
Audit Classes	Editar el archivo audit_class. Consulte audit_class(4).	Audit Control
Audit Control	Editar el archivo audit_control. Consulte audit_control(4).	Audit Control
Audit Events	Editar el archivo audit_event. Consulte audit_event(4).	Audit Control
Audit Startup	Editar la secuencia de comandos audit_startup.sh. Consulte audit_startup(1M).	Audit Control
Check Encodings	Ejecutar el comando chk_encodings en el archivo de codificaciones especificado. Consulte chk_encodings(1M).	Object Label Management
Check TN Files	Ejecutar el comando tnchkdb en las bases de datos tnrhdb, tnrhtp y tnzonecfg. Consulte tnchkdb(1M).	Gestión de redes
Configure Selection Confirmation	Editar el archivo /usr/dt/config/sel_config. Consulte sel_config(4).	Object Label Management
Create LDAP Client	Convertir la zona global en un cliente LDAP de un servicio de directorios LDAP existente.	Information Security
Edit Encodings	Editar el archivo label_encodings especificado y ejecutar el comando chk_encodings. Consulte chk_encodings(1M).	Object Label Management

TABLA 2–2 Acciones administrativas en Trusted CDE, su finalidad y los perfiles de derechos asociados *(Continuación)*

Nombre de la acción	Finalidad de la acción	Perfil de derechos predeterminado
`Name Service Switch`	Editar el archivo `nsswitch.conf`. Consulte `nsswitch.conf(4)`.	Gestión de redes
`Set DNS Servers`	Editar el archivo `resolv.conf`. Consulte `resolv.conf(4)`.	Gestión de redes
`Set Daily Message`	Editar el archivo `/etc/motd`. En el inicio de sesión, los contenidos de este archivo aparecen en el cuadro de diálogo Last Login.	Gestión de redes
`Set Default Routes`	Especificar rutas estáticas predeterminadas.	Gestión de redes
`Share Filesystem`	Editar el archivo `dfstab`. Esta acción no ejecuta el comando `share`. Consulte `dfstab(4)`.	Gestión del sistema de archivos

El equipo de configuración inicial utiliza las siguientes acciones durante la creación de zonas. Algunas de estas acciones pueden utilizarse para mantenimiento y resolución de problemas.

TABLA 2–3 Acciones de instalación en Trusted CDE, su finalidad y los perfiles de derechos asociados

Nombre de la acción	Finalidad de la acción	Perfil de derechos predeterminado
`Clone Zone`	Crear una zona con etiquetas de una instantánea de ZFS de una zona existente.	Zone Management
`Copy Zone`	Crear una zona con etiquetas desde una zona existente.	Zone Management
`Configure Zone`	Asociar una etiqueta con un nombre de zona.	Zone Management
`Initialize Zone for LDAP`	Inicializar la zona para iniciar como cliente LDAP.	Zone Management
`Install Zone`	Instalar los archivos del sistema que una zona con etiquetas necesita.	Zone Management
`Restart Zone`	Reiniciar una zona que ya se ha iniciado.	Zone Management
`Share Logical Interface`	Configurar una interfaz para la zona global y una interfaz independiente para que las zonas con etiquetas compartan.	Gestión de redes
`Share Physical Interface`	Configurar una interfaz para que la compartan la zona global y las zonas con etiquetas.	Gestión de redes
`Shut Down Zone`	Cerrar una zona instalada.	Zone Management
`Start Zone`	Iniciar una zona instalada y los servicios para dicha zona.	Zone Management
`Zone Terminal Console`	Abrir una consola para ver los procesos de una zona instalada.	Zone Management

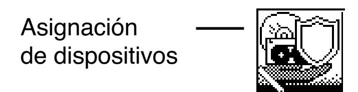
Device Allocation Manager

Un *dispositivo* es un periférico físico que está conectado a un equipo o un dispositivo simulado mediante software que se llama *pseudodispositivo*. Dado que los dispositivos proporcionan un medio para la importación y la exportación de datos de un sistema a otro, estos deben controlarse a fin de proteger los datos de manera adecuada. Trusted Extensions utiliza rangos de etiquetas de dispositivos y asignación de dispositivos para controlar los datos que fluyen por los dispositivos.

Entre los dispositivos que tienen rangos de etiquetas se encuentran los búferes de trama, las unidades de cinta, las unidades de disquetes y CD-ROM, las impresoras y los dispositivos USB.

Los usuarios asignan dispositivos mediante Device Allocation Manager. Device Allocation Manager monta el dispositivo, ejecuta una secuencia de comandos clean para prepararlo y realiza la asignación. Una vez terminado esto, el usuario desasigna el dispositivo mediante Device Allocation Manager, que ejecuta otra secuencia de comandos clean y desmonta y desasigna el dispositivo.

FIGURA 2–1 Icono de Device Allocation Manager en Trusted CDE



Puede gestionar dispositivos con la herramienta Device Administration de Device Allocation Manager. Los usuarios comunes no tienen acceso a Device Allocation Manager.

Nota – En Solaris Trusted Extensions (JDS), esta interfaz gráfica de usuario se denomina Device Manager, y el botón de Device Administration se denomina Administration.

FIGURA 2–2 Interfaz gráfica de usuario de Device Allocation Manager



Para obtener más información sobre la protección de dispositivos en Trusted Extensions, consulte el Capítulo 17, "Gestión de dispositivos para Trusted Extensions (tareas)".

Herramientas de Solaris Management Console

Solaris Management Console proporciona acceso a las cajas de herramientas de administración basadas en la interfaz gráfica de usuario. Estas herramientas permiten editar opciones de distintas bases de datos de configuración. En Trusted Extensions, Solaris Management Console es la interfaz administrativa para los usuarios, los roles y las bases de datos de la red de confianza.

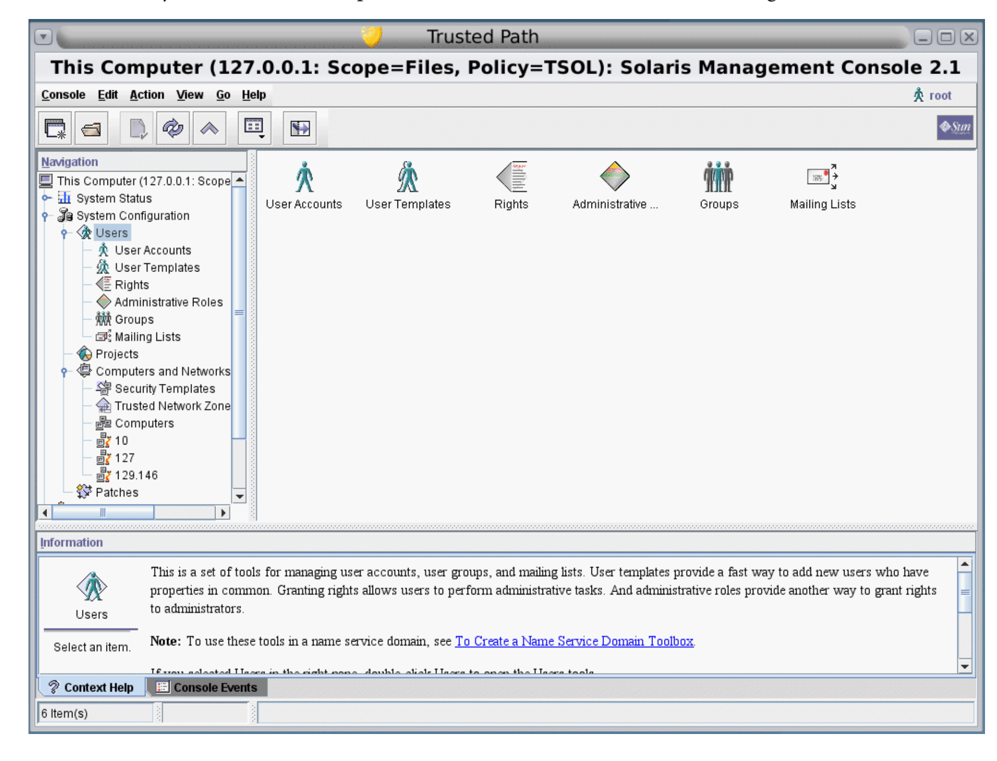
Trusted Extensions amplía Solaris Management Console:

- Trusted Extensions modifica el conjunto de herramientas Users de Solaris Management Console. Para ver una introducción al conjunto de herramientas, consulte el Capítulo 2, "Trabajo con Solaris Management Console (tareas)" de *Administración de Oracle Solaris: administración básica*.
- Trusted Extensions agrega las herramientas Security Templates y Trusted Network Zones al conjunto de herramientas Computers and Networks.

Las herramientas de Solaris Management Console se reúnen en *cajas de herramientas* según el ámbito y la política de seguridad. Para administrar Trusted Extensions, Trusted Extensions proporciona cajas de herramientas con `Policy=TSOL`. Puede acceder a las herramientas en función del ámbito, es decir, según el servicio de nombres. Los ámbitos disponibles son el host local y LDAP.

En la siguiente figura, se ve una imagen de Solaris Management Console. Aparece cargada una caja de herramientas `Scope=Files` de Trusted Extensions, y el conjunto de herramientas Users está abierto.

FIGURA 2–3 Caja de herramientas típica de Trusted Extensions en Solaris Management Console



Herramientas de Trusted Extensions en Solaris Management Console

Trusted Extensions proporciona atributos de seguridad que pueden configurarse para tres herramientas:

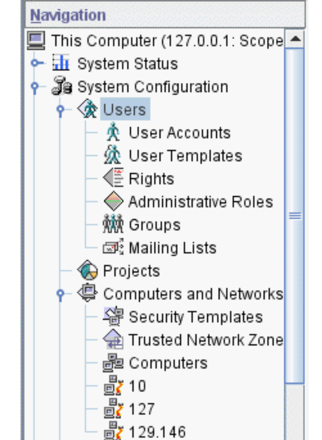
- **Herramienta User Accounts**: es la interfaz administrativa que permite cambiar las etiquetas de usuarios y la visualización de las etiquetas que tiene el usuario, y también controlar el uso de la cuenta.
- **Herramienta Administrative Roles**: es la interfaz administrativa que permite cambiar el comportamiento de bloqueo de pantalla y el rango de etiquetas de los roles durante el tiempo de inactividad.
- **Herramienta Rights**: incluye acciones de CDE que pueden asignarse a perfiles de derechos. Los atributos de seguridad pueden asignarse a estas acciones.

Trusted Extensions agrega dos herramientas al conjunto Computers and Networks:

- **Herramienta Security Templates**: es la interfaz administrativa que permite gestionar aspectos relativos a las etiquetas de los hosts y las redes. Esta herramienta modifica las bases de datos `tnrhtp` y `tnrhdb`, aplica la precisión sintáctica y actualiza el núcleo con los cambios.
- **Herramienta Trusted Network Zones**: es la interfaz administrativa que sirve para gestionar los aspectos relativos a las etiquetas de las zonas. Esta herramienta modifica la base de datos `tnzonecfg`, aplica la precisión sintáctica y actualiza el núcleo con los cambios.

La Figura 2–4 muestra la caja de herramientas Files con el conjunto de herramientas Users resaltado. Las herramientas de Trusted Extensions aparecen debajo del conjunto de herramientas Computers and Networks.

FIGURA 2–4 Conjunto de herramientas Computers and Networks definido en Solaris Management Console



Herramienta Security Templates

La *plantilla de seguridad* describe un conjunto de atributos de seguridad que pueden asignarse a un grupo de hosts. La herramienta Security Templates le permite asignar adecuadamente una combinación específica de atributos de seguridad a un grupo de hosts. Estos atributos controlan el modo en que los datos se empaquetan, se transmiten y se interpretan. Los hosts que se asignan a una plantilla tienen las mismas configuraciones de seguridad.

Los hosts se definen en la herramienta Computers. Los atributos de seguridad de los hosts se asignan en la herramienta Security Templates. El cuadro de diálogo Modify Template contiene dos fichas:

- **Ficha General**: describe la plantilla. Incluye el nombre, el tipo de host, la etiqueta predeterminada, el dominio de interpretación (DOI, Domain of Interpretation), el rango de acreditación y el conjunto de etiquetas de sensibilidad discretas.
- **Ficha Hosts Assigned to Template**: enumera todos los hosts de la red que asignó a esta pantalla.

Las redes de confianza y las plantillas de seguridad se explican en más detalle en el Capítulo 12, “Redes de confianza (descripción general)”.

Herramienta Trusted Network Zones

La herramienta Trusted Network Zones identifica las zonas del sistema. Al inicio, la zona global aparece en la lista. Cuando agrega zonas con sus etiquetas, los nombres de las zonas se muestran en el panel. Por lo general, la creación de zonas se produce durante la configuración del sistema. La asignación de etiquetas, la configuración de puertos de varios niveles y la política de etiquetas se configuran en esta herramienta. Para obtener detalles, consulte el Capítulo 10, “Gestión de zonas en Trusted Extensions (tareas)”.

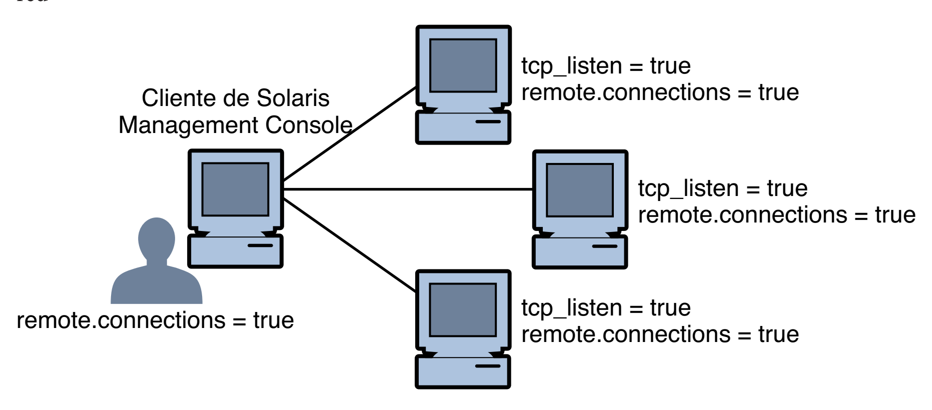
Comunicación cliente-servidor con Solaris Management Console

Normalmente, el cliente de Solaris Management Console administra los sistemas *de manera remota*. En una red que utiliza LDAP como servicio de nombres, el cliente de Solaris Management Console se conecta con el servidor de Solaris Management Console que se ejecuta en el servidor LDAP. La siguiente figura muestra esta configuración.

FIGURA 2–5 Cliente de Solaris Management Console que usa un servidor LDAP para administrar la red

La Figura 2–6 muestra una red que no está configurada con un servidor LDAP. El administrador configuró cada sistema remoto con un servidor de Solaris Management Console.

FIGURA 2–6 Cliente de Solaris Management Console que administra sistemas remotos individuales en una red

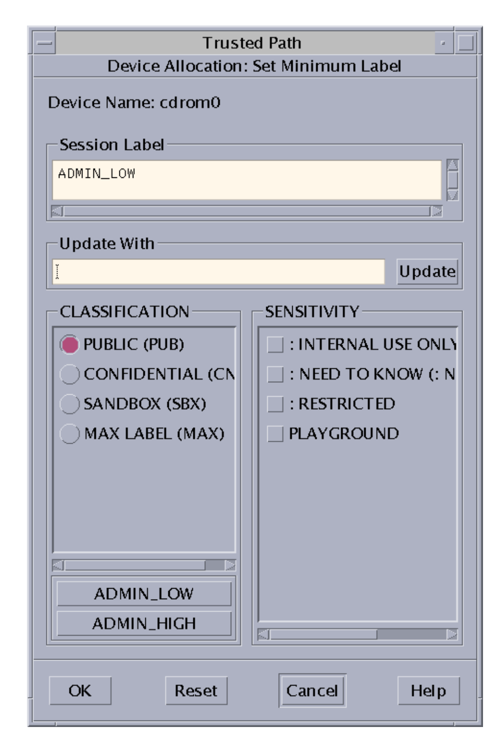


Documentación de Solaris Management Console

La principal fuente de documentación de Solaris Management Console es la ayuda en pantalla. La ayuda contextual aparece en el panel de información y está enlazada con la función que se encuentre seleccionada. Para acceder a los temas de ayuda ampliada, vaya al menú Help o haga clic en los enlaces de la ayuda contextual. Se proporciona más información en el Capítulo 2, "Trabajo con Solaris Management Console (tareas)" de *Administración de Oracle Solaris: administración básica*. También consulte "Uso de las herramientas de gestión de Solaris con RBAC (mapa de tareas)" de *Administración de Oracle Solaris: administración básica*.

Generador de etiquetas en Trusted Extensions

La interfaz gráfica de usuario del generador de etiquetas aplica la etiqueta válida o la acreditación que usted elija cuando un programa le solicite que asigne una etiqueta. Por ejemplo, un generador de etiquetas aparece durante el inicio de sesión (consulte el Capítulo 2, "Logging In to Trusted Extensions (Tasks)" de *Trusted Extensions User's Guide*). El generador de etiquetas también aparece cuando cambia la etiqueta de un espacio de trabajo o cuando asigna una etiqueta a un usuario, una zona o una interfaz de red en Solaris Management Console. El siguiente generador de etiquetas aparece cuando asigna un rango de etiquetas a un nuevo dispositivo.



En el generador de etiquetas, los nombres de los componentes en la columna Classification corresponden a la sección `CLASSIFICATIONS` del archivo `label_encodings`. Los nombres de los componentes de la columna Sensitivity corresponden a la sección `WORDS` en el archivo `label_encodings`.

Herramientas de la línea de comandos en Trusted Extensions

Los comandos que son exclusivos de Trusted Extensions se incluyen en el *Manual de referencia de Trusted Extensions*. Los comandos de Oracle Solaris que Trusted Extensions modifica se incluyen en el *Manual de referencia de Oracle Solaris*. El comando `man` busca todos los comandos.

La siguiente tabla enumera los comandos que son exclusivos de Trusted Extensions. Los comandos se enumeran en el formato de la página del comando man.

TABLA 2–4 Comandos de usuario y de administración de Trusted Extensions

Página del comando man	Modificación de Trusted Extensions	Para obtener más información
`add_allocatable`(1M)	Permite que los dispositivos se asignen mediante la agregación del dispositivo a las bases de datos de asignación de dispositivos. De manera predeterminada, los dispositivos extraíbles se pueden asignar.	"Cómo configurar un dispositivo en Trusted Extensions" en la página 247
`atohexlabel`(1M)	Convierte una etiqueta en formato hexadecimal.	"Cómo obtener el equivalente hexadecimal de una etiqueta" en la página 73
`chk_encodings`(1M)	Comprueba la integridad del archivo `label_encodings`.	"How to Debug a label_encodings File" de *Trusted Extensions Label Administration*
`dtappsession`(1)	Abre una sesión remota de Trusted CDE con Application Manager.	Capítulo 8, "Administración remota en Trusted Extensions (tareas)"
`getlabel`(1)	Muestra la etiqueta de los archivos o directorios seleccionados.	"Cómo visualizar las etiquetas de los archivos montados" en la página 133
`getzonepath`(1)	Muestra el nombre de ruta completo de una zona específica.	"Acquiring a Sensitivity Label" de *Trusted Extensions Developer's Guide*
`hextoalabel`(1M)	Convierte una etiqueta hexadecimal en su equivalente en lenguaje natural.	"Cómo obtener una etiqueta legible de su forma hexadecimal" en la página 74
`plabel`(1)	Muestra la etiqueta del proceso actual.	Consulte la página del comando man.
`remove_allocatable`(1M)	Impide la asignación de un dispositivo mediante la eliminación de su entrada de las bases de datos de asignación de dispositivos.	"Cómo configurar un dispositivo en Trusted Extensions" en la página 247
`setlabel`(1)	Vuelve a etiquetar el elemento seleccionado. Requiere las autorizaciones `solaris.label.file.downgrade` o `solaris.label.file.upgrade`. Estas autorizaciones están en el perfil de derechos de gestión de etiquetas de objetos.	Para conocer el procedimiento de GUI equivalente, consulte "How to Move Files Between Labels in Trusted CDE" de *Trusted Extensions User's Guide*.

TABLA 2–4 Comandos de usuario y de administración de Trusted Extensions *(Continuación)*

Página del comando man	Modificación de Trusted Extensions	Para obtener más información
smtnrhdb(1M)	Gestiona las entradas de la base de datos tnrhdb localmente o en una base de datos de servicios de nombres.	Para conocer los procedimientos equivalentes que utilizan Solaris Management Console, consulte "Configuración de bases de datos de red de confianza (mapa de tareas)" en la página 182.
smtnrhtp(1M)	Gestiona las entradas de la base de datos tnrhtp localmente o en una base de datos de servicios de nombres.	Consulte la página del comando man.
smtnzonecfg(1M)	Gestiona las entradas de la base de datos tnzonecfg local.	Para conocer un procedimiento equivalente que usa Solaris Management Console, consulte "Cómo crear un puerto de varios niveles para una zona" en la página 141.
tnchkdb(1M)	Comprueba la integridad de las bases de datos tnrhdb y tnrhtp.	"Cómo comprobar la sintaxis de las bases de datos de red de confianza" en la página 198
tnctl(1M)	Almacena en caché la información de red en el núcleo.	"Cómo sincronizar la caché del núcleo con las bases de datos de red de confianza" en la página 200
tnd(1M)	Ejecuta el daemon de la red de confianza.	"Cómo sincronizar la caché del núcleo con las bases de datos de red de confianza" en la página 200
tninfo(1M)	Muestra la información de red del nivel del núcleo y las estadísticas.	"Cómo comparar la información de la base de datos de red de confianza con la caché del núcleo" en la página 198.
updatehome(1M)	Actualiza los archivos .copy_files y .link_files para la etiqueta actual.	"Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 90

En la siguiente tabla, se enumeran los comandos de Oracle Solaris que se modifican o se amplían mediante Trusted Extensions. Los comandos se enumeran en el formato de la página del comando man.

TABLA 2–5 Comandos de usuario y de administración que Trusted Extensions modifica

Página del comando man	Modificación de Trusted Extensions	Para obtener más información
`allocate`(1)	Agregar opciones para limpiar el dispositivo asignado y para asignar un dispositivo a una zona específica. En Trusted Extensions, los usuarios comunes no utilizan este comando.	"How to Allocate a Device in Trusted Extensions" de *Trusted Extensions User's Guide*
`deallocate`(1)	Agregar opciones para limpiar el dispositivo y para desasignar un dispositivo de una zona específica. En Trusted Extensions, los usuarios comunes no utilizan este comando.	"How to Allocate a Device in Trusted Extensions" de *Trusted Extensions User's Guide*
`list_devices`(1)	Agrega la opción `-a` para mostrar los atributos del dispositivo, como las autorizaciones y las etiquetas. Agrega la opción `-d` para mostrar los atributos predeterminados de un tipo de dispositivo asignado. Agrega la opción `-z` para mostrar los dispositivos disponibles que pueden asignarse a una zona con etiquetas.	Consulte la página del comando man.
`tar`(1)	Agrega la opción `-T` para archivar y extraer los archivos y directorios que tengan etiquetas.	"Cómo realizar copias de seguridad de los archivos en Trusted Extensions" en la página 152 y "Cómo restaurar archivos en Trusted Extensions" en la página 153
`auditconfig`(1M)	Agregar las opciones de política de auditoría `windata_down` y `windata_up`.	"How to Configure Audit Policy" de *System Administration Guide: Security Services*
`auditreduce`(1M)	Agrega la opción `-l` para seleccionar los registros de auditoría por etiqueta.	"How to Select Audit Events From the Audit Trail" de *System Administration Guide: Security Services*
`automount`(1M)	Modificar los nombres y los contenidos de los mapas `auto_home` para justificar los nombres y la visibilidad de la zona de etiquetas superiores.	"Cambios en el montador automático en Trusted Extensions" en la página 150
`ifconfig`(1M)	Agregar la opción `all-zones` opción para que una interfaz esté a disposición en todas las zonas del sistema.	"Cómo verificar que las interfaces del host estén activas" en la página 202
`netstat`(1M)	Agregar la opción `-R` para mostrar los atributos de seguridad ampliados para los sockets y las entradas de la tabla de enrutamiento.	"Cómo depurar la red de Trusted Extensions" en la página 203
`route`(1M)	Agregar la opción `-secattr` para mostrar los atributos de seguridad de la ruta: `cipso`, `doi`, `max_sl` y `min_sl`.	"Cómo configurar las rutas con los atributos de seguridad" en la página 196

Administración remota en Trusted Extensions

Para administrar remotamente un sistema configurado con Trusted Extensions, debe utilizar el comando `ssh`, el programa `dtappsession` o Solaris Management Console. Si la política de seguridad del sitio lo permite, puede configurar un host de Trusted Extensions para activar el inicio de sesión desde un host que no sea de Trusted Extensions, aunque esta configuración sea menos segura. Para obtener información, consulte el Capítulo 8, "Administración remota en Trusted Extensions (tareas)".



CAPÍTULO 3

Introducción para administradores de Trusted Extensions (tareas)

Este capítulo brinda una introducción a la administración de sistemas que están configurados con Trusted Extensions.

Novedades de Trusted Extensions

Solaris 10 1/13: en esta versión, Trusted Extensions agrega eventos de auditoría para el subsistema de impresión. Lea el archivo `/etc/security/audit_event` para conocer la definición de los eventos de impresión confianza `AUE_print_request`, `AUE_print_request_ps`, `AUE_print_request_unlabeled` y `AUE_print_request_nobanner`.

Solaris 10 10/08 – En esta versión, Trusted Extensions proporciona las siguientes funciones:

- La pila IP compartida de Trusted Extensions permite que las rutas predeterminadas aíslen las zonas con etiquetas entre sí y también las aíslen de la zona global.
- La interfaz de bucle de retorno, `lo0`, es una interfaz `all-zones`.
- La separación de tareas puede aplicarse por rol. El rol de administrador del sistema crea usuarios, pero no puede asignar contraseñas. El rol de administrador de la seguridad asigna contraseñas, pero no puede crear usuarios. Para obtener detalles, consulte "Create Rights Profiles That Enforce Separation of Duty" de *Trusted Extensions Configuration Guide*.
- Esta guía incluye una lista de las páginas del comando man de Trusted Extensions en el Apéndice B, "Lista de las páginas del comando man de Trusted Extensions".

Solaris 10 5/08 – En esta versión, Trusted Extensions proporciona las siguientes funciones:

- La utilidad de gestión de servicios (SMF) administra Trusted Extensions como el servicio `svc:/system/labeld`. De manera predeterminada, el servicio `labeld` está desactivado. Cuando el servicio está activado, se debe configurar y reiniciar el sistema para aplicar las políticas de seguridad de Trusted Extensions.
- El número de dominio de interpretación (DOI) de opción de seguridad de IP comercial (CIPSO, Commercial IP Security Option) que su sistema utiliza puede configurarse.
  - Para obtener más información sobre el dominio de interpretación, consulte "Atributos de seguridad de red en Trusted Extensions" en la página 168.
  - Para especificar un dominio de interpretación que sea diferente del que está predeterminado, consulte "Configure the Domain of Interpretation" de *Trusted Extensions Configuration Guide*.
- Trusted Extensions reconoce las etiquetas CIPSO en los sistemas de archivos montados en la versión 3 de NFS (NFSv3) y también en la versión 4 de NFS (NFSv4). Por lo tanto, puede montar sistemas de archivos NFSv3 en un sistema Trusted Extensions como sistema de archivos con etiquetas. Para utilizar udp como protocolo subyacente para montajes de varios niveles en NFSv3, consulte "Cómo configurar un puerto de varios niveles para NFSv3 mediante `udp`" en la página 141.
- El daemon de la caché del servicio de nombres, `nscd`, puede configurarse para que se ejecute en cada zona con etiquetas en la etiqueta de la zona.

Requisitos de seguridad para la administración de Trusted Extensions

En Trusted Extensions, los roles son el medio convencional para administrar el sistema. Por lo general, el superusuario no se utiliza. Los roles se crean iguales a los del SO Oracle Solaris, y la mayoría de las tareas se realizan mediante roles. En Trusted Extensions, el usuario `root` no se utiliza para realizar las tareas administrativas.

Los siguientes son los roles típicos de un sitio de Trusted Extensions:

- **Rol** `root`: creado por el equipo de configuración inicial
- **Rol de administrador de la seguridad**: creado por el equipo de configuración inicial durante, o una vez finalizada, la configuración inicial.
- **Rol de administrador del sistema**: creado por el rol de administrador de la seguridad

Como en el SO Oracle Solaris, también puede crear un rol de administrador principal, un rol de operador, etc. A excepción del rol `root`, puede administrar en un servicio de nombres los roles que cree.

Como en el SO Oracle Solaris, solamente los usuarios que tiene un rol asignado pueden asumir ese rol. En Solaris Trusted Extensions (CDE), puede asumir un rol desde el menú de escritorio

llamado Trusted Path Menu. En Solaris Trusted Extensions (JDS), puede asumir un rol cuando su nombre de usuario se muestra en la banda de confianza. Las opciones del rol aparecen al hacer clic en el nombre de usuario.

Creación de roles en Trusted Extensions

Para administrar Trusted Extensions, puede crear roles que dividan las funciones del sistema y de la seguridad. El equipo de configuración inicial creó el rol de administrador de la seguridad durante la configuración. Para obtener detalles, consulte "Create the Security Administrator Role in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

El proceso de creación de roles en Trusted Extensions es idéntico al proceso del SO Oracle Solaris. Como se describe en el Capítulo 2, "Herramientas de administración de Trusted Extensions", Solaris Management Console es la interfaz gráfica de usuario para administrar roles en Trusted Extensions.

- Para obtener una descripción general de la creación de roles, consulte el Capítulo 10, "Role-Based Access Control (Reference)" de *System Administration Guide: Security Services* y "Using RBAC (Task Map)" de *System Administration Guide: Security Services*.
- Para crear un rol eficaz que sea equivalente a un superusuario, consulte "Creación del rol de administrador principal" de *Administración de Oracle Solaris: administración básica*. En los sitios que usan Trusted Extensions, el rol de administrador principal pueden infringir la política de seguridad. Estos sitios convertirían al usuario `root` en un rol y crearían un rol de administrador de la seguridad.
- Para crear el rol `root`, consulte "How to Make root User Into a Role" de *System Administration Guide: Security Services*.
- Para crear roles con Solaris Management Console, consulte "How to Create and Assign a Role by Using the GUI" de *System Administration Guide: Security Services*.

Asunción de roles en Trusted Extensions

A diferencia del SO Oracle Solaris, Trusted Extensions proporciona la opción de menú Assume *Rolename* Role desde el menú Trusted Path. Después de confirmar la contraseña del rol, el software activa un espacio de trabajo para el rol con el atributo de la ruta de confianza. Los espacios de trabajo de rol son espacios de trabajo administrativos. Estos espacios de trabajo se encuentran en la zona global.

Introducción para administradores de Trusted Extensions (mapa de tareas)

Familiarícese con los siguientes procedimientos antes de administrar Trusted Extensions.

Tarea	Descripción	Para obtener instrucciones
Iniciar sesión.	Permite iniciar sesión de manera segura.	"Logging In to Trusted Extensions" de *Trusted Extensions User's Guide*
Realizar tareas de usuario comunes en un escritorio.	Entre las tareas, se incluye lo siguiente: ■ Configurar los espacios de trabajo ■ Usar espacios de trabajo en diferentes etiquetas ■ Acceder a las páginas del comando man de Trusted Extensions ■ Acceder a la ayuda en línea de Trusted Extensions	"Working on a Labeled System" de *Trusted Extensions User's Guide*
Realizar tareas que requieren la ruta de confianza.	Entre las tareas, se incluye lo siguiente: ■ Asignar un dispositivo ■ Cambiar la contraseña ■ Cambiar la etiqueta de un espacio de trabajo	"Performing Trusted Actions" de *Trusted Extensions User's Guide*
Crear roles útiles.	Crear roles administrativos para el sitio. La creación de roles en LDAP se realiza una sola vez. El rol de administrador de la seguridad es un rol útil.	"Creación de roles en Trusted Extensions" en la página 51 "Create the Security Administrator Role in Trusted Extensions" de *Trusted Extensions Configuration Guide*
(Opcional) Convierta un rol en `root`.	Impedir el inicio de sesión anónimo de `root`. Esta tarea se realiza una sola vez por sistema.	"How to Make root User Into a Role" de *System Administration Guide: Security Services*
Asuma un rol.	Introducir la zona global en un rol. Todas las tareas administrativas se realizan en la zona global.	"Cómo entrar en la zona global en Trusted Extensions" en la página 53
Salir del espacio de trabajo de un rol y convertirse en usuario común.	Dejar la zona global.	"Cómo salir de la zona global en Trusted Extensions" en la página 54
Administrar usuarios, roles, derechos, zonas y redes en el ámbito local.	Utilizar Solaris Management Console para administrar el sistema distribuido.	"Cómo administrar el sistema local con Solaris Management Console" en la página 55

Tarea	Descripción	Para obtener instrucciones
Administrar el sistema mediante las acciones Trusted CDE.	Utilizar las acciones administrativas en la carpeta Trusted_Extensions.	"Cómo iniciar acciones administrativas de CDE en Trusted Extensions" en la página 56
Editar un archivo administrativo.	Editar archivos en un editor de confianza.	"Cómo editar archivos administrativos en Trusted Extensions" en la página 57
Administrar la asignación de dispositivos.	Utilizar la interfaz gráfica de usuario Device Allocation Manager – Device Administration.	"Gestión de dispositivos en Trusted Extensions (mapa de tareas)" en la página 246

▼ Cómo entrar en la zona global en Trusted Extensions

Cuando asume un rol, entra en la zona global en Trusted Extensions. Es posible administrar todo el sistema solamente desde la zona global. Sólo los superusuarios o los roles pueden entrar en la zona global.

Después de que se asume un rol, con él se puede crear un espacio de trabajo en una etiqueta de usuario a fin de editar los archivos administrativos en una zona con etiquetas.

Para la resolución de problemas, también puede entrar en la zona global si inicia una sesión en modo a prueba de fallos. Para obtener detalles, consulte "Cómo iniciar una sesión en modo a prueba de fallos en Trusted Extensions" en la página 93.

Antes de empezar Debe haber creado uno o más roles, o estar por entrar en la zona global como superusuario. Para obtener referencias, consulte "Creación de roles en Trusted Extensions" en la página 51.

1 Use un mecanismo de confianza.

- **En Solaris Trusted Extensions (JDS), haga clic en su nombre de usuario en la banda de confianza y seleccione un rol.**

  Si se le asignó un rol, los nombres de rol se muestran en una lista.

  Para conocer sobre la ubicación y la importancia de las funciones de escritorio de Trusted Extensions, consulte el Capítulo 4, "Elements of Trusted Extensions (Reference)" de *Trusted Extensions User's Guide*.

- **En Solaris Trusted Extensions (CDE), abra el menú Trusted Path.**

  a. **Haga clic con el tercer botón del mouse en el área de selección de espacios de trabajo.**



  b. **Seleccione Assume** *rolename* **Role del menú Trusted Path.**

2 Cuando se solicite, escriba la contraseña de rol.

En Trusted CDE, se crea un nuevo espacio de trabajo de rol, el botón de selección de espacios de trabajo se cambia al color del escritorio del rol, y la barra de título de cada ventana muestra el título `Trusted Path`. En Trusted JDS, el espacio de trabajo actual cambia al espacio de trabajo del rol.

En Trusted CDE, si desea salir del espacio de trabajo de un rol, debe usar el mouse para seleccionar el espacio de trabajo de un usuario común. También puede suprimir el último espacio de trabajo de rol para salir de un rol. En Trusted JDS, debe hacer clic en el nombre de rol en la banda de confianza, y luego seleccionar del menú un rol o usuario diferente. Esta acción cambia el espacio de trabajo actual al proceso del nuevo rol o usuario.

▼ Cómo salir de la zona global en Trusted Extensions

Las ubicaciones del menú para salir de un rol son diferentes en Trusted JDS y en Trusted CDE.

Antes de empezar Debe encontrarse en la zona global.

● **En ambos escritorios, puede hacer clic en el espacio de trabajo de un usuario en el área de selección de espacios de trabajo.**

También puede salir del espacio de trabajo del rol, y por consiguiente de la zona global, si realiza una de las siguientes acciones:

- **En Trusted JDS, haga clic en el nombre del rol en la banda de confianza.**

  Al hacer clic en el nombre del rol, aparece su nombre de usuario y una lista con los roles que puede asumir. Si selecciona su nombre de usuario, todas las ventanas que cree en lo sucesivo

en ese espacio de trabajo tendrán el nombre seleccionado. Las ventanas que haya creado anteriormente en el escritorio actual seguirán apareciendo con el nombre y la etiqueta del rol.

Si selecciona un nombre de rol diferente, permanecerá en la zona global con un rol diferente.

- **En Trusted CDE, suprima el espacio de trabajo del rol.**

  Haga clic con el tercer botón del mouse sobre el botón del espacio de trabajo y seleccione Delete. Volverá al último espacio de trabajo que había ocupado.

▼ Cómo administrar el sistema local con Solaris Management Console

La primera vez que Solaris Management Console se inicia en un sistema, se produce un retraso mientras se registran las herramientas y se crean los distintos directorios. Por lo general, este retraso se produce durante la configuración del sistema. Para conocer el procedimiento, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

Para saber cómo administrar un sistema remoto, consulte "Administración remota de Trusted Extensions (mapa de tareas)" en la página 108.

Antes de empezar Debe haber asumido un rol. Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 53.

1 **Inicie Solaris Management Console.**

En Solaris Trusted Extensions (JDS), utilice la línea de comandos.

```
$ /usr/sbin/smc &
```

En Trusted CDE, tiene tres opciones.

- **Utilice el comando `smc` en una ventana de terminal.**
- **En el menú desplegable Tools del panel frontal, haga clic en el icono de Solaris Management Console.**
- **En la carpeta Trusted_Extensions, haga doble clic en el icono de Solaris Management Console.**

2 **Seleccione Console -> Open Toolbox.**

3 **En la lista, seleccione una caja de herramientas de Trusted Extensions del ámbito adecuado.**

La caja de herramientas de Trusted Extensions incluye `Policy=TSOL` en su nombre. El ámbito Files actualiza los archivos locales en el sistema actual. El ámbito LDAP actualiza los directorios LDAP en Oracle Directory Server Enterprise Edition. Los nombres de las cajas de herramientas serán similares a los siguientes:

```
This Computer (this-host: Scope=Files, Policy=TSOL)
This Computer (ldap-server: Scope=LDAP, Policy=TSOL)
```

4 **Vaya hasta la herramienta de Solaris Management Console que desee.**

Se muestra el indicador de contraseña.

Para las herramientas que Trusted Extensions haya modificado, haga clic en System Configuration.

5 **Escriba la contraseña del usuario.**

Consulte la ayuda en pantalla para obtener información adicional sobre las herramientas de Solaris Management Console. Para obtener una introducción a las herramientas que Trusted Extensions modifica, consulte "Herramientas de Solaris Management Console" en la página 38.

6 **Para cerrar la interfaz gráfica de usuario, seleccione Exit en el menú Console.**

▼ Cómo iniciar acciones administrativas de CDE en Trusted Extensions

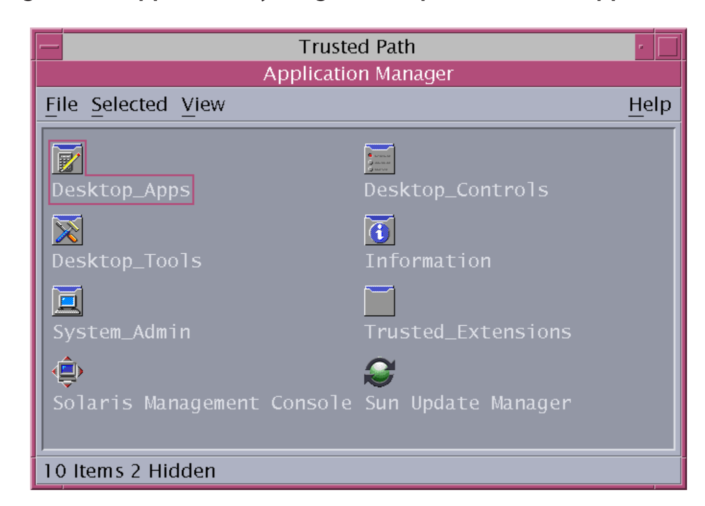
1 **Asuma un rol.**

Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 53.

2 **En Trusted CDE, traiga Application Manager hacia adelante.**

a. **Haga clic con el tercer botón del mouse en el fondo para que aparezca el menú Workspace.**

b. **Haga clic en Applications y, luego, en la opción de menú Application Manager.**



La carpeta Trusted_Extensions está en Application Manager.

3 **Abra la carpeta Trusted_Extensions.**

4 **Haga doble clic en el icono adecuado.**

Para obtener una lista de las acciones administrativas, consulte "Acciones de Trusted CDE" en la página 35.

▼ Cómo editar archivos administrativos en Trusted Extensions

Los archivos administrativos se editan con un editor de confianza que incorpora la auditoría. Este editor también impide que el usuario ejecute los comandos del shell o que guarde con un nombre de archivo que no sea el nombre del archivo original.

1 **Asuma un rol.**

Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 53.

2 **Abra un editor de confianza.**

- **En Solaris Trusted Extensions (CDE), realice lo siguiente:**

  a. **A fin de traer el editor hacia adelante, haga clic con el tercer botón del mouse en el fondo para que aparezca el menú Workspace.**

b. **Haga clic en Applications y, luego, en la opción de menú Application Manager.**

La carpeta Trusted_Extensions está en Application Manager.

c. **Abra la carpeta Trusted_Extensions.**

d. **Haga doble clic en la acción Admin Editor.**

Se le indicará que proporcione un nombre de archivo. Para ver el formato, consulte el Paso 3 y el Paso 4.

- **En Solaris Trusted Extensions (JDS), realice lo siguiente:**
  - **(Opcional) Para usar `gedit` como editor de confianza, modifique la variable `EDITOR`.**

    Para obtener detalles, consulte "Cómo asignar el editor de su elección como editor de confianza" en la página 70.
  - **Utilice la línea de comandos para traer el editor de confianza hacia adelante.**

    ```
    # /usr/dt/bin/trusted_edit filename
    ```

    Debe proporcionar un argumento *filename*.

3 **Para crear un archivo nuevo, escriba el nombre de ruta completo del archivo nuevo.**

Cuando guarde el archivo, el editor creará un archivo temporal.

4 **Para editar un archivo existente, escriba el nombre de ruta completo del archivo existente.**

Nota – Si su editor proporciona la opción de guardar como, no la utilice. Utilice la opción de guardar del editor para guardar el archivo.

---

5 **Para guardar el archivo en el nombre de ruta especificado, cierre el editor.**



CAPÍTULO 4

Requisitos de seguridad del sistema Trusted Extensions (descripción general)

En este capítulo, se describen las funciones de seguridad que pueden configurarse en un sistema con Trusted Extensions.

Funciones de seguridad de Oracle Solaris que pueden configurarse

Trusted Extensions utiliza las mismas funciones de seguridad que proporciona el SO Oracle Solaris y agrega algunas otras funciones. Por ejemplo, el SO Oracle Solaris proporciona protección `eeprom`, algoritmos de contraseña complejos y requisitos de contraseña, protección del sistema mediante el bloqueo del usuario, y protección frente a la interrupción del teclado.

Trusted Extensions difiere del SO Oracle Solaris en los procedimientos concretos que se utilizan para modificar estos valores predeterminados de seguridad. En Trusted Extensions, normalmente se asume un rol para administrar los sistemas. Las configuraciones locales se modifican con el editor de confianza. Los cambios que afectan la red de usuarios, roles y hosts se realizan en Solaris Management Console.

Interfaces de Trusted Extensions para configurar las funciones de seguridad

En esta guía, se mencionan procedimientos en que Trusted Extensions requiere una interfaz específica para modificar la configuración de seguridad. Dicha interfaz es opcional en el SO Oracle Solaris. En esta guía, no se mencionan procedimientos por separado en los que Trusted

Extensions requiera el uso del editor de confianza para editar archivos locales. Por ejemplo, el procedimiento "Cómo impedir el bloqueo de cuentas de los usuarios" en la página 100 describe cómo actualizar una cuenta de usuario con Solaris Management Console para impedir el bloqueo de la cuenta. Sin embargo, el procedimiento de configuración de la política de bloqueo de contraseña de todo el sistema no se proporciona en esta guía. Siga las instrucciones de Oracle Solaris, salvo que esté en Trusted Extensions, utilice el editor de confianza para modificar el archivo del sistema.

Ampliación de los mecanismos de seguridad de Oracle Solaris por Trusted Extensions

Los siguientes mecanismos de seguridad de Oracle Solaris pueden ampliarse en Trusted Extensions como se amplían en el SO Oracle Solaris:

- **Clases y eventos de auditoría**: la agregación de clases y eventos de auditoría se describe en el Capítulo 30, "Managing Oracle Solaris Auditing (Tasks)" de *System Administration Guide: Security Services*.
- **Perfiles de derechos**: la agregación de perfiles de derechos se describe en la Parte III, "Roles, Rights Profiles, and Privileges" de *System Administration Guide: Security Services*.
- **Roles**: la agregación de roles se describe en la Parte III, "Roles, Rights Profiles, and Privileges" de *System Administration Guide: Security Services*.
- **Autorizaciones**: para ver un ejemplo de agregación de una nueva autorización, consulte "Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 257.

Como en el SO Oracle Solaris, los privilegios no se pueden ampliar.

Funciones de seguridad de Trusted Extensions

Trusted Extensions proporciona las siguientes funciones de seguridad exclusivas:

- **Etiquetas**: los sujetos y los objetos tienen etiquetas. Los procesos tienen etiquetas. Las zonas y la red tienen etiquetas.
- **Device Allocation Manager**: de manera predeterminada, los dispositivos se encuentran protegidos por los requisitos de asignación. La GUI de Device Allocation Manager es la interfaz para administradores y para usuarios comunes.
- **Opción de menú Change Password**: el menú Trusted Path le permite cambiar su contraseña de usuario y la contraseña del rol que asumió.

Aplicación de los requisitos de seguridad

A fin de garantizar que la seguridad del sistema no se vea comprometida, los administradores necesitan proteger las contraseñas, los archivos y los datos de auditoría. Los usuarios deben estar capacitados para hacer su parte del trabajo. Para cumplir con los requisitos de una configuración evaluada, siga las directrices descritas de esta sección.

Usuarios y requisitos de seguridad

Cada administrador de la seguridad del sitio debe garantizar que los usuarios reciban la formación necesaria sobre procedimientos de seguridad. El administrador de la seguridad necesita comunicar las siguientes reglas a los empleados nuevos y recordarlas a los empleados existentes con regularidad:

- No diga a nadie la contraseña.

  Cualquiera que conozca su contraseña puede acceder a la misma información que usted sin identificarse y, por lo tanto, sin tener que responsabilizarse.
- No escriba su contraseña en un papel ni la incluya en un correo electrónico.
- Elija contraseñas que sean difíciles de adivinar.
- No envíe su contraseña a nadie por correo electrónico.
- No deje su equipo desatendido sin bloquear la pantalla o cerrar sesión.
- Recuerde que los administradores no dependen del correo electrónico para enviar instrucciones a los usuarios. Nunca siga las instrucciones enviadas mediante correo electrónico por un administrador sin antes confirmar con el administrador.

  Tenga en cuenta que la información del remitente en el correo electrónico puede falsificarse.
- Dado que es responsable de los permisos de acceso a los archivos y directorios que crea, asegúrese de que los permisos de los archivos y directorios se hayan definido correctamente. No permita que los usuarios no autorizados lean o modifiquen un archivo, enumeren los contenidos de un directorio, o aumenten un directorio.

Es posible que en su sitio desee proporcionar sugerencias adicionales.

Uso del correo electrónico

Utilizar el correo electrónico para dar instrucciones a los usuarios de que realicen alguna acción resulta una práctica insegura.

Diga a los usuarios que no confíen en los correos electrónicos que contienen instrucciones que provienen presuntamente de un administrador. De este modo, se evita la posibilidad de que se envíen mensajes de correo electrónico falsos con el objeto de engañar a los usuarios para que cambien la contraseña a un valor determinado o para que la divulguen, lo que posteriormente podría ser utilizado para iniciar sesión y poner en riesgo el sistema.

Aplicación de la contraseña

El rol de administrador del sistema debe especificar un nombre de usuario y un ID de usuario únicos al crear una nueva cuenta. Cuando selecciona el nombre y el ID de una nueva cuenta, el administrador debe asegurarse de que tanto el nombre de usuario como el ID asociado no se encuentren duplicados en ninguna parte de la red ni se hayan utilizado previamente.

El rol de administrador de la seguridad tiene la responsabilidad de especificar la contraseña original para cada cuenta y de comunicar las contraseñas a los usuarios de cuentas nuevas. Debe tener en cuenta la siguiente información al administrar las contraseñas:

- Asegúrese de que las cuentas para los usuarios que pueden asumir el rol de administrador de la seguridad se hayan configurado de manera que la cuenta no se pueda bloquear. Esta práctica garantiza que al menos una cuenta siempre pueda iniciar sesión y asumir el rol de administrador de la seguridad para volver a abrir las cuentas de todos los demás si estas se bloquean.
- Comunique la contraseña al usuario de una cuenta nueva de modo tal que nadie más pueda enterarse de cuál es la contraseña.
- Cambie la contraseña de una cuenta ante la más mínima sospecha de que alguien que no debiera conocer la contraseña la haya descubierto.
- Nunca use los nombres de usuario o los ID de usuario más de una vez durante la vida útil del sistema.

  Al asegurarse de que los nombres de usuario y los ID de usuario no se vuelvan a utilizar, se evitan posibles confusiones respecto de lo siguiente:

  - Las acciones que realizó cada usuario en el análisis de los registros de auditoría
  - Los archivos que posee cada usuario en la restauración de archivos

Protección de la información

Como administrador, tiene la responsabilidad de configurar y mantener correctamente la protección del control de acceso discrecional (DAC) y del control de acceso obligatorio (MAC) para los archivos cuya seguridad es crítica. Entre los archivos críticos, se incluyen los siguientes:

- **Archivo** `shadow`: contiene contraseñas cifradas. Consulte `shadow`(4).
- **Base de datos** `prof_attr`: contiene definiciones de los perfiles de derechos. Consulte `prof_attr`(4).
- **Base de datos** `exec_attr`: contiene los comandos y las acciones que forman parte de los perfiles de derechos. Consulte `exec_attr`(4).
- **Archivo** `user_attr`: contiene los perfiles de derechos, los privilegios y las autorizaciones que están asignadas a los usuarios locales. Consulte `user_attr`(4).

- **Pista de auditoría**: contiene los registros de auditoría que el servicio de auditoría ha recopilado. Consulte `audit.log(4)`



Precaución – Dado que los mecanismos de protección para las entradas LDAP no están sujetos a la política de control de acceso que aplica el software de Trusted Extensions, las entradas LDAP predeterminadas no deben ampliarse, y sus reglas de acceso no deben modificarse.

Protección de contraseña

En los archivos locales, la protección que evita la visualización de las contraseñas se realiza mediante DAC, y la que evita su modificación, mediante DAC y MAC. Las contraseñas de las cuentas locales se actualizan en el archivo `/etc/shadow`, que solamente el superusuario puede leer. Para obtener más información, consulte la página del comando man `shadow(4)`.

Administración de grupos

El rol de administrador del sistema necesita comprobar, en el sistema local y en la red, que todos los grupos tengan un único ID de grupo (GID, Group ID).

Cuando se suprime del sistema un grupo local, el rol de administrador del sistema debe garantizar que:

- Todos los objetos con el GID del grupo eliminado se deben suprimir o asignar a otro grupo.
- A todos los usuarios que tienen el grupo suprimido como grupo principal se les asigne otro grupo principal.

Prácticas de supresión de usuarios

Cuando se suprime una cuenta del sistema, el rol de administrador del sistema y el rol de administrador de la seguridad deben realizar las siguientes acciones:

- Suprimir los directorios principales de la cuenta en cada zona.
- Suprimir cualquier proceso o trabajo que pertenezca a la cuenta eliminada:
  - Suprimir cualquier objeto que pertenezca a la cuenta o asignar la propiedad a otro usuario.
  - Suprimir cualquier trabajo de `at` o `batch` planificado en nombre del usuario. Para obtener detalles, consulte las páginas del comando man `at(1)` y `crontab(1)`.
- Nunca vuelva a usar el nombre de usuario (cuenta) ni el ID de usuario.

Reglas para cambiar el nivel de seguridad de los datos

De manera predeterminada, los usuarios comunes pueden emplear las operaciones de cortar y pegar, copiar y pegar, y arrastrar y soltar en los archivos y en las selecciones. El origen y el destino deben estar en la misma etiqueta.

Para cambiar la etiqueta de los archivos o la etiqueta de la información dentro de los archivos se requiere autorización. Cuando los usuarios están autorizados a cambiar el nivel de seguridad de los datos, la aplicación Selection Manager media en la transferencia. En Trusted CDE, el archivo `/usr/dt/config/sel_config` controla las acciones para volver a etiquetar archivos y para cortar o copiar la información, y pegarla en una etiqueta diferente. En Trusted JDS, el archivo `/usr/share/gnome/sel_config` controla estas transferencias. En Trusted CDE, la aplicación `/usr/dt/bin/sel_mgr` controla las operaciones de arrastrar y soltar entre las ventanas. Como se muestra en las siguientes tablas, hay más restricciones para volver a etiquetar una selección que un archivo.

La siguiente tabla muestra un resumen de las reglas para volver a etiquetar archivos. Las reglas incluyen las operaciones de cortar y pegar, copiar y pegar, y arrastrar y soltar.

TABLA 4–1 Condiciones para mover archivos a una etiqueta nueva

Descripción de la transacción	Relaciones de etiquetas	Relaciones de propietarios	Autorización requerida
Copiar y pegar, cortar y pegar, o arrastrar y soltar archivos entre administradores de archivos	Misma etiqueta	Mismo UID	None (Nada)
	Disminución de nivel	Mismo UID	`solaris.label.file.downgrade`
	Actualización	Mismo UID	`solaris.label.file.upgrade`
	Disminución de nivel	Diferentes UID	`solaris.label.file.downgrade`
	Actualización	Diferentes UID	`solaris.label.file.upgrade`

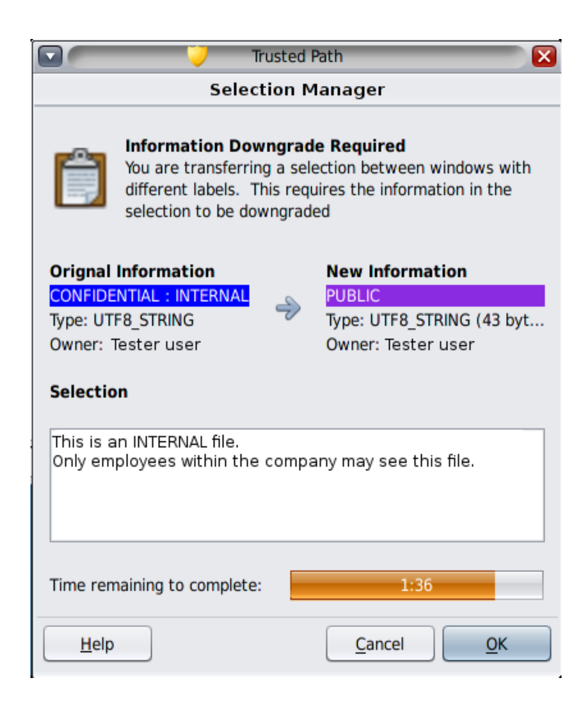
Se aplican reglas diferentes a las selecciones en una ventana que en un archivo. La acción de arrastrar y soltar *selecciones* siempre requiere que exista igualdad de etiquetas y propiedad. La acción de arrastrar y soltar entre ventanas es mediada por la aplicación Selection Manager, no por el archivo `sel_config`.

Las reglas para cambiar la etiqueta de selecciones se resumen en la siguiente tabla.

TABLA 4–2 Condiciones para mover selecciones a una etiqueta nueva

Descripción de la transacción	Relaciones de etiquetas	Relaciones de propietarios	Autorización requerida
Copiar y pegar, o cortar y pegar selecciones entre ventanas	Misma etiqueta	Mismo UID	None (Nada)
	Disminución de nivel	Mismo UID	`solaris.label.win.downgrade`
	Actualización	Mismo UID	`solaris.label.win.upgrade`
	Disminución de nivel	Diferentes UID	`solaris.label.win.downgrade`
	Actualización	Diferentes UID	`solaris.label.win.upgrade`
Arrastrar y soltar las selecciones entre las ventanas	Misma etiqueta	Mismo UID	Ninguna

Trusted Extensions proporciona un confirmador de selección para que medie en los cambios de etiquetas. Esta ventana aparece cuando un usuario autorizado intenta cambiar la etiqueta de un archivo o selección. El usuario tiene 120 segundos para confirmar la operación. Para cambiar el nivel de seguridad de datos sin esta ventana, se requiere la autorización `solaris.label.win.noview` además de que se vuelvan a etiquetar las autorizaciones. La siguiente ilustración muestra una selección (`zonename`) en la ventana.



De manera predeterminada, el confirmador de selección aparece cuando se transfieren datos a una etiqueta diferente. Si una selección requiere varias decisiones de transferencia, el mecanismo de respuesta automático proporciona un modo de responder una sola vez a todas las transferencias. Para obtener más información, consulte la página del comando man sel_config(4) y la sección siguiente.

Archivo sel_config

El archivo sel_config se verifica a fin de determinar la conducta del confirmador de selección cuando una operación aumente o disminuya el nivel de una etiqueta.

El archivo sel_config define lo siguiente:

- Qué tipos de selecciones obtienen respuestas automáticas
- Qué tipos de operaciones pueden confirmarse automáticamente
- Cuándo se muestra un cuadro de diálogo del confirmador de selección

En Trusted CDE, el rol de administrador de la seguridad puede cambiar los valores predeterminados con la acción Configure Selection Confirmation en la carpeta Trusted_Extensions. Los nuevos valores entran en vigor en el siguiente inicio de sesión. En Solaris Trusted Extensions (JDS), la acción de CDE no está disponible. Para cambiar los valores predeterminados, modifique el archivo /usr/share/gnome/sel_config en un editor de texto.

Personalización de Solaris Trusted Extensions (CDE)

En Solaris Trusted Extensions (CDE), los usuarios pueden agregar acciones al panel frontal y personalizar el menú Workspace. El software de Trusted Extensions limita la capacidad de los usuarios para agregar programas y comandos a CDE.

Personalización del panel frontal

Cualquier usuario puede arrastrar una acción preexistente de Application Manager y soltarla en el panel frontal, siempre que la cuenta que realiza la modificación tenga la acción en su perfil. Se pueden agregar al panel frontal las acciones de los directorios /usr/dt/ o /etc/dt/, pero no las aplicaciones del directorio $HOME/.dt/appconfig. Aunque los usuarios pueden utilizar la acción Create Action, no pueden escribir en cualquiera de los directorios donde se almacenan las acciones de todo el sistema. Por lo tanto, los usuarios comunes no pueden crear acciones que sean utilizables.

En Trusted Extensions, se cambió la ruta de búsqueda de las acciones. Las acciones del directorio principal de cualquier usuario individual no se procesan al principio, sino a lo último. Por lo tanto, nadie puede personalizar las acciones existentes.

Al rol de administrador de la seguridad se le asigna la acción Admin Editor para que pueda realizar las modificaciones necesarias en el archivo `/usr/dt/appconfig/types/C/dtwm.fp` y en los demás archivos de configuración para los subpaneles del panel frontal.

Personalización del menú Workspace

El menú Workspace aparece al hacer clic con el tercer botón del mouse en el fondo del espacio de trabajo. Los usuarios comunes pueden personalizar el menú y agregarle opciones.

Cuando se permite al usuario trabajar en varias etiquetas, se aplican las condiciones siguientes:

- El usuario debe tener un directorio principal en la zona global.

  Para guardar las personalizaciones, los procesos de la zona global deben poder escribir en la etiqueta correcta del directorio principal del usuario. La ruta de la zona al directorio principal de un usuario en la que los procesos de la zona global pueden escribir es similar a la siguiente:

  `/zone/`*zone-name*`/home/`*username*
- El usuario debe usar las opciones Customize Menu y Add Item to Menu en el espacio de trabajo de un usuario común. El usuario puede crear una personalización diferente para cada etiqueta.
- Cuando el usuario asume un rol, los cambios en el menú Workspace persisten.
- Los cambios que se realizan en el menú Workspace se almacenan en el directorio principal del usuario en la etiqueta actual. El archivo de menú personalizado es `.dt/wsmenu`.
- El perfil de derechos del usuario debe permitir al usuario ejecutar la acción deseada.

  Cualquier acción que se agregue al menú Workspace debe gestionarse mediante uno de los perfiles de derechos del usuario. De lo contrario, la acción falla cuando se la invoca, y aparece un mensaje de error.

  Por ejemplo, cualquier usuario que tenga la acción Run puede hacer doble clic en el icono de cualquier ejecutable para ejecutarlo, incluso si la acción o algún comando que la acción invoca no están incluidos en los perfiles de derechos de las cuentas. De manera predeterminada, los roles no tienen asignada la acción Run. Por lo tanto, cualquier opción de menú que requiera la acción Run falla cuando la ejecuta un rol.



CAPÍTULO 5

Administración de los requisitos de seguridad en Trusted Extensions (tareas)

Este capítulo trata las tareas que se realizan normalmente en el sistema configurado con Trusted Extensions.

Tareas comunes en Trusted Extensions (mapa de tareas)

En el siguiente mapa de tareas, se describen los procedimientos que configuran el entorno de trabajo para los administradores de Trusted Extensions.

Tarea	Descripción	Para obtener instrucciones
Cambiar el programa editor del editor de confianza.	Especificar el editor para los archivos administrativos.	"Cómo asignar el editor de su elección como editor de confianza" en la página 70
Cambiar la contraseña de root.	Especificar una contraseña nueva para el usuario `root` o el rol `root`.	"Cómo cambiar la contraseña de `root`" en la página 71
Cambiar la contraseña de un rol.	Especificar una contraseña nueva para el rol actual.	Ejemplo 5–2
Utilizar la combinación de teclas de aviso de seguridad.	Permite obtener control del mouse o el teclado. Además, permite probar si el mouse o el teclado son de confianza.	"Cómo recuperar el control del enfoque actual del escritorio" en la página 72
Determinar el número hexadecimal de una etiqueta.	Muestra la representación interna de una etiqueta de texto.	"Cómo obtener el equivalente hexadecimal de una etiqueta" en la página 73
Determinar la representación de texto de una etiqueta.	Muestra la representación de texto de una etiqueta hexadecimal.	"Cómo obtener una etiqueta legible de su forma hexadecimal" en la página 74
Editar archivos del sistema.	Edita de manera segura los archivos del sistema de Oracle Solaris o Trusted Extensions.	"Cómo cambiar los valores predeterminados de seguridad en los archivos del sistema" en la página 75

Tarea	Descripción	Para obtener instrucciones
Asignar un dispositivo.	Utiliza un dispositivo periférico para agregar o eliminar información en el sistema.	"How to Allocate a Device in Trusted Extensions" de *Trusted Extensions User's Guide*
Administrar un host de manera remota.	Administra hosts de Oracle Solaris o Trusted Extensions desde un host remoto.	Capítulo 8, "Administración remota en Trusted Extensions (tareas)"

▼ Cómo asignar el editor de su elección como editor de confianza

El editor de confianza utiliza el valor de la variable de entorno `$EDITOR` como editor.

Antes de empezar Debe estar en un rol de la zona global.

1 Determine el valor de la variable `$EDITOR`.

```
# echo $EDITOR
```

A continuación se mencionan los editores posibles. También es posible que la variable `$EDITOR` no se establezca.

- `/usr/dt/bin/dtpad`: es el editor que CDE proporciona.
- `/usr/bin/gedit`: es el editor que Java Desktop System, versión *number* proporciona. Solaris Trusted Extensions (JDS) es la versión de confianza de ese escritorio.
- `/usr/bin/vi`: es el editor visual.

2 Establezca el valor de la variable `$EDITOR`.

- **Para definir el valor de manera permanente, modifique el valor en el archivo de inicialización del shell del rol.**

  Por ejemplo, en el directorio principal del rol, modifique el archivo `.kshrc` en un shell Korn y el archivo `.cshrc` en un shell C.

- **Para definir el valor del shell actual, establézcalo en la ventana de terminal.**

  Por ejemplo, en un shell Korn, utilice los siguientes comandos:

  ```
  # setenv EDITOR=pathname-of-editor
  # export $EDITOR
  ```

  En un shell C, utilice el siguiente comando:

  ```
  # setenv EDITOR=pathname-of-editor
  ```

En un shell Bourne, utilice los siguientes comandos:

```
# EDITOR=pathname-of-editor
# export EDITOR
```

Ejemplo 5–1 Especificación del editor como editor de confianza

El rol de administrador de la seguridad desea utilizar `vi` para editar los archivos del sistema. El usuario que asume el rol modifica el archivo de inicialización `.kshrc` en el directorio principal del rol.

```
$ cd /home/secadmin
$ vi .kshrc

## Interactive shell
set -o vi
...
export EDITOR=vi
```

La próxima vez que un usuario asuma el rol de administrador de la seguridad, `vi` será el editor de confianza.

▼ Cómo cambiar la contraseña de root

El rol de administrador de la seguridad está autorizado a cambiar la contraseña de una cuenta en cualquier momento mediante Solaris Management Console. Sin embargo, no se puede cambiar la contraseña de una cuenta del sistema mediante Solaris Management Console. La *cuenta del sistema* es una cuenta que tiene un UID inferior a 100. `root` es una cuenta del sistema porque su UID es 0.

1. **Conviértase en superusuario.**

   Si su sitio determinó el superusuario en el rol `root`, asuma el rol `root`.

2. **Seleccione Change Password en el menú Trusted Path.**

   - **En Trusted JDS, haga clic en el símbolo de confianza de la banda de confianza.**

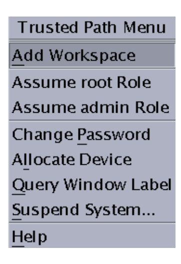
     En el menú Trusted Path, elija Change Password.

     Trusted I tester CONFIDENTIAL : INTERNAL USE ONLY Trusted Path
     Change Password...
     Allocate Device...
     Query Window Label...
     Help...

   - **En Solaris Trusted Extensions (CDE), abra el menú Trusted Path.**

     a. **Haga clic con el tercer botón del mouse en el área de selección de espacios de trabajo.**

b. Seleccione Change Password en el menú Trusted Path.



3 Cambie la contraseña y confirme el cambio.

Ejemplo 5–2 Cambio de la contraseña de un rol

Cualquier usuario que pueda asumir un rol definido en LDAP puede utilizar el menú Trusted Path para cambiar la contraseña del rol. La contraseña de todos los usuarios que intentan asumir el rol se cambia en LDAP.

Como en el SO Oracle Solaris, el rol de administrador principal puede cambiar la contraseña de un rol mediante Solaris Management Console. En Trusted Extensions, el rol de administrador de la seguridad puede cambiar la contraseña de otro rol mediante Solaris Management Console.

▼ Cómo recuperar el control del enfoque actual del escritorio

La combinación de teclas de aviso de seguridad se puede utilizar para interrumpir un arrastre del puntero o del teclado que provenga de una aplicación que no sea de confianza. Esta combinación de teclas también puede utilizarse para verificar si un arrastre del puntero o del teclado proviene de una aplicación de confianza. En un sistema de varios periféricos que se ha suplantado para que se muestre más de una banda de confianza, esta combinación de teclas dirige el puntero hacia la banda de confianza autorizada.

1 Para recuperar el control de un teclado de Sun, utilice la siguiente combinación de teclas.

Presione las teclas simultáneamente para recuperar el control del enfoque actual del escritorio. En el teclado de Sun, el rombo es la tecla Meta.

```
<Meta> <Stop>
```

Si el arrastre, como un puntero, no es de confianza, el puntero se mueve hacia la banda. Si el puntero es de confianza, no se pasa a la banda de confianza.

2 Si no utiliza un teclado de Sun, use la siguiente combinación de teclas.

```
<Alt> <Break>
```

Presione las teclas simultáneamente para recuperar el control del enfoque del escritorio actual de su equipo portátil.

Ejemplo 5–3 Comprobar si la petición de contraseña es de confianza

En un sistema x86 que se usa con un teclado de Sun, se le solicita una contraseña al usuario. Se arrastra el puntero y se lo ubica en el cuadro de diálogo de contraseña. Para comprobar si el indicador es de confianza, el usuario presiona simultáneamente las teclas <Meta> y <Stop>. Cuando el puntero permanece en el cuadro de diálogo, el usuario sabe que la petición de contraseña es de confianza.

Si el puntero se mueve a la banda de confianza, el usuario se da cuenta de que la petición de contraseña no es de confianza, por lo que debe ponerse en contacto con el administrador.

Ejemplo 5–4 Forzar el puntero hacia la banda de confianza

En este ejemplo, un usuario no está ejecutando ningún proceso de confianza, pero no puede ver el puntero del mouse. Para ubicar el puntero en el centro de la banda de confianza, el usuario presiona simultáneamente las teclas <Meta> y <Stop>.

▼ Cómo obtener el equivalente hexadecimal de una etiqueta

Este procedimiento proporciona la representación hexadecimal interna de una etiqueta. Esta representación se puede almacenar con seguridad en un directorio público. Para obtener más información, consulte la página del comando man `atohexlabel`(1M).

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global. Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 53.

● **Para obtener el valor hexadecimal de una etiqueta, realice una de las acciones siguientes.**

- **Para obtener el valor hexadecimal de una etiqueta de sensibilidad, pase la etiqueta al comando.**

```
$ atohexlabel "CONFIDENTIAL : NEED TO KNOW"
0x0004-08-68
```

- **Para obtener el valor hexadecimal de una acreditación, utilice la opción `-c`.**

```
$ atohexlabel -c "CONFIDENTIAL NEED TO KNOW"
0x0004-08-68
```

Nota – Las etiquetas de sensibilidad y de acreditación en lenguaje natural se forman según las reglas del archivo `label_encodings`. Cada tipo de etiqueta utiliza reglas de una sección independiente de este archivo. Cuando la etiqueta de sensibilidad y la etiqueta de acreditación expresan el mismo nivel de sensibilidad subyacente, ambas tienen una forma hexadecimal idéntica. Sin embargo, las etiquetas pueden tener diferentes formas en lenguaje natural. Las interfaces del sistema que aceptan etiquetas en lenguaje natural como entrada esperan un tipo de etiqueta. Si las cadenas de texto de los tipos de etiquetas difieren, estas cadenas de texto no se pueden intercambiar.

En el archivo predeterminado `label_encodings`, el equivalente de texto de una etiqueta de acreditación no incluye dos puntos (:).

Ejemplo 5–5 Uso del comando `atohexlabel`

Cuando pasa una etiqueta válida en formato hexadecimal, el comando devuelve el argumento.

```
$ atohexlabel 0x0004-08-68
0x0004-08-68
```

Cuando pasa una etiqueta administrativa, el comando devuelve el argumento.

```
$ atohexlabel admin_high
ADMIN_HIGH
atohexlabel admin_low
ADMIN_LOW
```

Errores más frecuentes El mensaje de error `atohexlabel parsing error found in <string> at position 0` indica que el argumento `<string>` que pasó a `atohexlabel` no es una etiqueta o acreditación válidas. Verifique que no haya errores de escritura y compruebe que la etiqueta exista en el archivo `label_encodings` que tiene instalado.

▼ Cómo obtener una etiqueta legible de su forma hexadecimal

Este procedimiento proporciona un modo de reparar las etiquetas almacenadas en las bases de datos internas. Para obtener más información, consulte la página del comando man `hextoalabel`(1M).

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **Para obtener el equivalente de texto de la representación interna de una etiqueta, realice una de las acciones siguientes.**

  - **Para obtener el equivalente de texto de una etiqueta de sensibilidad, pase la forma hexadecimal de la etiqueta.**

    ```
    $ hextoalabel 0x0004-08-68
    CONFIDENTIAL : NEED TO KNOW
    ```

  - **Para obtener el equivalente de texto de una acreditación, utilice la opción -c.**

    ```
    $ hextoalabel -c 0x0004-08-68
    CONFIDENTIAL NEED TO KNOW
    ```

▼ Cómo cambiar los valores predeterminados de seguridad en los archivos del sistema

En Trusted Extensions, el administrador de la seguridad cambia las configuraciones de seguridad predeterminadas o accede a ellas en un sistema.

Los archivos de los directorios `/etc/security` y `/etc/default` contienen configuraciones de seguridad. En un sistema Oracle Solaris, el superusuario puede editar estos archivos. Para obtener información sobre la seguridad de Oracle Solaris, consulte el Capítulo 3, "Controlling Access to Systems (Tasks)" de *System Administration Guide: Security Services*.



Precaución – Reduzca los valores predeterminados de seguridad del sistema únicamente si la política de seguridad del sitio lo permite.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **Utilice el editor de confianza para editar el archivo del sistema.**

  Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

  La siguiente tabla muestra los archivos de seguridad y los parámetros de seguridad que se deben cambiar en los archivos.

Archivo	Tarea	Para obtener más información
`/etc/default/login`	Reducir el número permitido de intentos de introducción de contraseña.	Consulte el ejemplo de "How to Monitor All Failed Login Attempts" de *System Administration Guide: Security Services*. Página del comando man `passwd(1)`

Archivo	Tarea	Para obtener más información
/etc/default/kbd	Desactive la interrupción del teclado.	"How to Disable a System's Abort Sequence" de *System Administration Guide: Security Services* **Nota** – En los hosts que los administradores utilizan para realizar la depuración, la configuración predeterminada para KEYBOARD_ABORT permite el acceso al depurador del núcleo kadb. Para obtener más información sobre el depurador, consulte la página del comando man kadb(1M).
/etc/security/policy.conf	Solicitar un algoritmo más potente para las contraseñas de usuario. Eliminar un privilegio básico de todos los usuarios de este host. Restringir a los usuarios de este host a las autorizaciones de usuario de Solaris básico.	Página del comando man policy.conf(4)
/etc/default/passwd	Solicitar a los usuarios que cambien las contraseñas con frecuencia. Solicitar a los usuarios que creen contraseñas que sean extremadamente diferentes. Solicitar una contraseña de usuario más larga. Solicitar una contraseña que no se pueda encontrar en el diccionario.	Página del comando man passwd(1)



◆ ◆ ◆ CAPÍTULO 6

Usuarios, derechos y roles en Trusted Extensions (descripción general)

En este capítulo, se explican las decisiones fundamentales que debe tomar antes de crear usuarios comunes y se proporciona información básica adicional para administrar las cuentas de usuario. En el capítulo, se supone que el equipo de configuración inicial ya configuró los roles y un número determinado de cuentas de usuario. Estos usuarios pueden asumir los roles que se utilizan para configurar y administrar Trusted Extensions. Para obtener detalles, consulte "Creating Roles and Users in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

Funciones de seguridad del usuario en Trusted Extensions

El software Trusted Extensions agrega las siguientes funciones de seguridad a usuarios, roles o perfiles de derechos:

- Los usuarios tienen un rango de etiquetas dentro del que pueden utilizar el sistema.
- Hay un rango de etiquetas dentro del que pueden utilizarse los roles para realizar tareas administrativas.
- Los perfiles de derecho de Trusted Extensions pueden incluir acciones administrativas de CDE. Como los comandos, las acciones pueden tener atributos de seguridad.
- Los comandos y las acciones en un perfil de derechos de Trusted Extensions tienen un atributo de etiqueta. Los comandos o las acciones deben realizarse dentro de un rango de etiquetas o en una etiqueta en particular.

- El software de Trusted Extensions agrega privilegios y autorizaciones al conjunto de privilegios y autorizaciones que el SO Oracle Solaris define.

Responsabilidades del administrador para los usuarios

El rol de administrador del sistema crea las cuentas de usuarios. El rol de administrador de la seguridad configura los aspectos de seguridad de una cuenta.

Si está utilizando Oracle Directory Server Enterprise Edition para el servicio de nombres LDAP, compruebe que el equipo de configuración inicial haya configurado la caja de herramientas `tsol_ldap.tbx`. Para conocer el procedimiento, consulte "Configuring the Solaris Management Console for LDAP (Task Map)" de *Trusted Extensions Configuration Guide*.

Para obtener detalles sobre la configuración de los usuarios y los roles, consulte lo siguiente:

- "Cómo crear el primer rol (administrador principal)" de *Administración de Oracle Solaris: administración básica*
- "Configuración de cuentas de usuario (mapa de tareas)" de *Administración de Oracle Solaris: administración básica*
- Parte III, "Roles, Rights Profiles, and Privileges" de *System Administration Guide: Security Services*

Responsabilidades del administrador del sistema para los usuarios

En Trusted Extensions, el rol de administrador del sistema es responsable de determinar quién puede acceder al sistema. El administrador del sistema es responsable de las siguientes tareas:

- Agregar y suprimir usuarios
- Agregar y suprimir roles
- Modificar las configuraciones de rol y de usuario que no sean atributos de seguridad

Responsabilidades del administrador de la seguridad para los usuarios

En Trusted Extensions, el rol de administrador de la seguridad es responsable de todos los atributos de seguridad de un usuario o rol. El administrador de la seguridad tiene a su cargo las siguientes tareas:

- Asignar y modificar los atributos de seguridad de un usuario, rol o perfil de derechos
- Crear y modificar perfiles de derechos
- Asignar perfiles de derechos a un usuario o rol
- Asignar privilegios a un usuario, rol o perfil de derechos
- Asignar autorizaciones a un usuario, rol o perfil de derechos
- Eliminar privilegios de un usuario, rol o perfil de derechos
- Eliminar autorizaciones de un usuario, rol o perfil de derechos

Normalmente, el rol de administrador de la seguridad crea perfiles de derechos. Sin embargo, si un perfil necesita capacidades que el rol de administrador de la seguridad no puede otorgar, el superusuario o el rol de administrador principal pueden crear el perfil.

Antes de crear un perfil de derechos, el administrador de la seguridad tiene que analizar si alguno de los comandos o las acciones en el perfil nuevo necesita un privilegio o una autorización para funcionar de manera correcta. Las páginas del comando man para los comandos individuales enumeran las autorizaciones y los privilegios que pueden necesitarse. Para ver ejemplos de acciones que requieren autorizaciones y privilegios, consulte la base de datos `exec_attr`.

Decisiones que deben tomarse antes de crear usuarios en Trusted Extensions

Las siguientes decisiones determinan lo que los usuarios pueden realizar en Trusted Extensions y cuánto deben esforzarse. Algunas decisiones son las mismas que deben tomarse cuando se instala el SO Oracle Solaris. Sin embargo, las decisiones que son específicas de Trusted Extensions pueden afectar la seguridad del sitio y la facilidad de uso.

- Decida si se cambian los atributos de seguridad del usuario predeterminados en el archivo `policy.conf`. Los valores predeterminados del usuario del archivo `label_encodings` fueron configurados por el equipo de configuración inicial. Para obtener una descripción de los valores predeterminados, consulte "Atributos de seguridad del usuario predeterminados en Trusted Extensions" en la página 80.

- Decida qué archivos de inicio se copiarán o enlazarán del directorio principal de etiqueta mínima del usuario a los directorios principales de nivel superior del usuario. Para conocer el procedimiento, consulte "Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 90.
- Decidir si los usuarios pueden acceder a los dispositivos periféricos, como el micrófono, el CD-ROM y la unidad Jaz.

  Si a algunos usuarios se les permite el acceso, decida si el sitio requiere autorizaciones adicionales a fin de garantizar la seguridad del sitio. Para obtener una lista predeterminada con las autorizaciones relacionadas con los dispositivos, consulte "Cómo asignar autorizaciones para dispositivos" en la página 261. Para ver un conjunto de autorizaciones de dispositivos más detallado, consulte "Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 257.

Atributos de seguridad del usuario predeterminados en Trusted Extensions

Las configuraciones de los archivos `label_encodings` y `policy.conf` definen conjuntamente los atributos de seguridad predeterminados para las cuentas de usuario. Los valores que establece explícitamente para un usuario sustituyen estos valores de sistema. Algunos valores que se establecen en estos archivos también se aplican a las cuentas de rol. Para conocer los atributos de seguridad que puede establecer explícitamente, consulte "Atributos de usuario que pueden configurarse en Trusted Extensions" en la página 81.

Valores predeterminados del archivo `label_encodings`

El archivo `label_encodings` define la visualización de la etiqueta predeterminada, la etiqueta mínima y la acreditación del usuario. Para obtener detalles sobre el archivo, consulte la página del comando man `label_encodings(4)`. El archivo `label_encodings` fue instalado por el equipo de configuración inicial. Las decisiones tomadas se basan en "Devising a Label Strategy" de *Trusted Extensions Configuration Guide* y ejemplos de *Trusted Extensions Label Administration* .

Los valores de las etiquetas que el administrador de la seguridad establece explícitamente para los usuarios individuales en Solaris Management Console derivan del archivo `label_encodings`. Los valores establecidos explícitamente sustituyen los valores del archivo `label_encodings`.

Valores predeterminados del archivo policy.conf en Trusted Extensions

El archivo /etc/security/policy.conf de Oracle Solaris contiene las configuraciones de seguridad predeterminadas para el sistema. Trusted Extensions agrega dos palabras clave a este archivo. Puede agregar estos pares palabra clave=valor al archivo si desea cambiar el valor de todo el sistema. Estas palabras clave se aplican mediante Trusted Extensions. La siguiente tabla muestra los valores posibles para estas configuraciones de seguridad y sus valores predeterminados.

TABLA 6–1 Valores predeterminados de seguridad de Trusted Extensions en el archivo policy.conf

Palabra clave	Valor predeterminado	Valores posibles	Notas
IDLECMD	LOCK	LOCK | LOGOUT	No se aplica a los roles.
IDLETIME	30	0 a 120 minutos	No se aplica a los roles.

Las autorizaciones y los perfiles de derechos que se definen en el archivo policy.conf son *adicionales* de cualquier autorización o perfil que se asigne a las cuentas individuales. Para los demás campos, el valor del usuario individual valor sustituye el valor del sistema.

En "Planning User Security in Trusted Extensions" de *Trusted Extensions Configuration Guide*, se incluye una tabla con todas las palabras clave de policy.conf. También, puede consultar la página del comando man policy.conf(4).

Atributos de usuario que pueden configurarse en Trusted Extensions

Para crear y modificar cuentas de usuario, debe usar Solaris Management Console 2.1. Para los usuarios que pueden iniciar sesión en más de una etiqueta, quizás desee configurar los archivos .copy_files y .link_files en el directorio principal de etiqueta mínima del usuario.

La herramienta User Accounts de Solaris Management Console funciona de la misma manera que en el SO Oracle Solaris, pero con dos excepciones:

- Trusted Extensions agrega atributos a las cuentas de usuario.
- El acceso al servidor del directorio principal requiere atención administrativa en Trusted Extensions.
  - Primero debe crear la entrada del servidor del directorio raíz igual que en el sistema Oracle Solaris.
  - Luego, el usuario y usted deben realizar los demás pasos para montar el directorio principal en cada etiqueta de usuario.

Como se describe en “Cómo agregar un usuario con la herramienta Users de Solaris Management Console” de *Administración de Oracle Solaris: administración básica*, un asistente le permite crear las cuentas de usuario con rapidez. Después de utilizar el asistente, puede modificar los atributos de Trusted Extensions predeterminados para el usuario.

Para obtener más información sobre los archivos `.copy_files` y `.link_files`, consulte “Archivos `.copy_files` y `.link_files`” en la página 84.

Atributos de seguridad que deben asignarse a los usuarios

El rol de administrador de la seguridad debe especificar algunos atributos de seguridad para los usuarios nuevos, como se muestra en la siguiente tabla. Para obtener información acerca de los archivos que contienen los valores predeterminados, consulte “Atributos de seguridad del usuario predeterminados en Trusted Extensions” en la página 80. La siguiente tabla muestra los atributos de seguridad que pueden asignarse a los usuarios y los efectos de cada asignación.

TABLA 6–2 Atributos de seguridad que se asignan después la creación del usuario

Atributo de usuario	Ubicación de valor predeterminado	Condición de la acción	Efecto de la acción
Contraseña	None (Nada)	Necesaria	El usuario tiene contraseña
Roles	None (Nada)	OPCIONAL	El usuario puede asumir un rol
Autorizaciones	Archivo `policy.conf`	OPCIONAL	El usuario tiene autorizaciones adicionales
Perfiles de derechos	Archivo `policy.conf`	OPCIONAL	El usuario tiene perfiles de derechos adicionales
Etiquetas	Archivo `label_encodings`	OPCIONAL	El usuario tiene un rango de acreditación o etiqueta predeterminado que es diferente
Con privilegios	Archivo `policy.conf`	OPCIONAL	El usuario tiene un conjunto de privilegios diferente
Uso de la cuenta	Archivo `policy.conf`	OPCIONAL	El usuario tiene una configuración diferente para cuando el equipo está inactivo
Auditoría	Archivo `audit_control`	OPCIONAL	El usuario se audita diferente que las configuraciones de auditoría del sistema

Asignación de atributos de seguridad a los usuarios en Trusted Extensions

El rol de administrador de la seguridad asigna los atributos de seguridad a los usuarios en Solaris Management Console una vez que se crean las cuentas de usuario. Si estableció los

valores predeterminados correctos, el siguiente paso consiste en asignar los atributos de seguridad únicamente a los usuarios que necesiten excepciones a los valores predeterminados.

Al asignar los atributos de seguridad a los usuarios, el administrador de la seguridad considera la siguiente información:

Asignación de contraseñas

El rol de administrador de la seguridad asigna contraseñas a las cuentas de usuario una vez que se crean las cuentas. Después de esta asignación inicial, los usuarios pueden cambiar sus contraseñas.

Como en el SO Oracle Solaris, se puede obligar a los usuarios a que cambien sus contraseñas periódicamente. Las opciones de caducidad de las contraseñas limitan el período durante el que un intruso capaz de adivinar o robar la contraseña puede acceder al sistema. Además, al establecer que transcurra un período mínimo antes de poder cambiar la contraseña, se impide que el usuario reemplace inmediatamente la contraseña nueva por la contraseña anterior. Para obtener detalles, consulte la página del comando man `passwd(1)`.

Nota – Las contraseñas de los usuarios que pueden asumir roles no deben estar sujetas a ninguna limitación por caducidad.

Asignación de roles

No es obligatorio que los usuarios tengan roles. Puede asignarse un solo usuario a más de un rol si esto concuerda con la política de seguridad del sitio.

Asignación de autorizaciones

Como en el SO Oracle Solaris, al asignar autorizaciones directamente a un usuario, se agregan autorizaciones nuevas a las existentes. En Trusted Extensions, primero se agregan las autorizaciones a un perfil de derechos y luego se asigna el perfil al usuario.

Asignación de perfiles de derechos

Como en el SO Oracle Solaris, el orden de los perfiles es importante. El mecanismo de los perfiles utiliza la primera instancia del comando o la acción del conjunto de perfiles de la cuenta.

Puede utilizar el orden de clasificación de perfiles para su beneficio. Si desea que un comando se ejecute con atributos de seguridad diferentes de los que se definen para el comando de un perfil existente, cree un perfil nuevo con las asignaciones preferidas para el comando. Luego, inserte ese perfil nuevo antes del perfil existente.

Nota – No asigne perfiles de derechos que incluyan acciones o comandos administrativos a un usuario común. Puede que el perfil no funcione porque el usuario común no puede entrar en la zona global.

Cambio de valores predeterminados de privilegios

El conjunto de privilegios predeterminado puede ser demasiado liberal para varios sitios. A fin de restringir el conjunto de privilegios para cualquier usuario común en el sistema, cambie la configuración del archivo `policy.conf`. Para cambiar el conjunto de privilegios de los usuarios individuales, utilice Solaris Management Console. Si desea obtener un ejemplo, consulte "Cómo restringir el conjunto de privilegios de un usuario" en la página 98.

Cambio de valores predeterminados de etiquetas

El cambio de los valores predeterminados de una etiqueta del usuario crea una excepción a los valores predeterminados del usuario en el archivo `label_encodings`.

Cambio de valores predeterminados de auditoría

Como en el SO Oracle Solaris, la asignación de clases de auditoría a un usuario crea excepciones a las clases de auditoría que se asignan en el archivo `/etc/security/audit_control` del sistema. Para obtener más información sobre auditoría, consulte el Capítulo 18, "Auditoría de Trusted Extensions (descripción general)".

Archivos `.copy_files` y `.link_files`

En Trusted Extensions, los archivos se copian automáticamente del directorio de estructura básica *sólo* en la zona que contiene la etiqueta mínima de la cuenta. A fin de garantizar que las zonas de las etiquetas superiores puedan usar los archivos de inicio, el usuario o el administrador deben crear los archivos `.copy_files` y `.link_files`.

Los archivos `.copy_files` y `.link_files` de Trusted Extensions ayudan a automatizar los procedimientos para copiar o enlazar los archivos de inicio en cada etiqueta del directorio principal de una cuenta. Siempre que un usuario crea un espacio de trabajo en una etiqueta nueva, el comando `updatehome` lee el contenido de `.copy_files` y `.link_files` en la etiqueta mínima de la cuenta. A continuación, el comando enlaza o copia cada archivo enumerado en el espacio de trabajo con etiquetas superiores.

El archivo `.copy_files` resulta útil cuando un usuario quiere que los archivos de inicio sean diferentes en las etiquetas diferentes. Se prefiere copiar, por ejemplo, cuando los usuarios utilizan alias de correo diferentes en etiquetas diferentes. El archivo `.link-files` resulta útil cuando es necesario que el archivo de inicio sea idéntico en cualquier etiqueta que se invoque. Se prefiere enlazar, por ejemplo, cuando una impresora se utiliza para todos los trabajos de impresión con etiquetas. Para ver archivos de ejemplo, consulte "Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 90.

La lista siguiente enumera algunos archivos de inicio que quizás quiera que los usuarios puedan enlazar o copiar en etiquetas superiores:

```
.acrorc          .dtprofile       .mailrc
.aliases         .emacs           .mime_types
.cshrc           .login           .newsrc
```

`.profile`	`.soffice`	`.Xdefaults-`*hostname*
`.signature`	`.Xdefaults`	



Gestión de usuarios, derechos y roles en Trusted Extensions (tareas)

En este capítulo se explican los procedimientos de Trusted Extensions para configurar y gestionar usuarios, cuentas de usuario y perfiles de derechos.

- "Personalización del entorno de usuario para la seguridad (mapa de tareas)" en la página 87
- "Gestión de usuarios y derechos con Solaris Management Console (mapa de tareas)" en la página 94
- "Manejo de otras tareas en Solaris Management Console (mapa de tareas)" en la página 102

Personalización del entorno de usuario para la seguridad (mapa de tareas)

En el siguiente mapa de tareas se describen las tareas comunes que puede llevar a cabo para personalizar un sistema para todos los usuarios o una cuenta de usuario individual.

Tarea	Descripción	Para obtener instrucciones
Cambiar los atributos de etiquetas.	Se modifican los atributos de etiquetas, como la vista de la etiqueta mínima y la etiqueta predeterminada, para una cuenta de usuario.	"Cómo modificar atributos de etiquetas de usuarios predeterminados" en la página 88

Tarea	Descripción	Para obtener instrucciones
Cambiar la política de Trusted Extensions para todos los usuarios de un sistema.	Se modifica el archivo `policy.conf`.	"Cómo modificar los valores predeterminados de `policy.conf`" en la página 89
	Activar el protector de pantalla después de transcurrido un período establecido. Cerrar la sesión del usuario cuando el sistema permanece inactivo durante un período establecido.	Ejemplo 7–1
	Eliminar los privilegios innecesarios de todos los usuarios comunes de un sistema.	Ejemplo 7–2
	Eliminar las etiquetas del resultado de la impresión en un quiosco público.	Ejemplo 7–3
Configurar los archivos de inicialización para los usuarios.	Configurar los archivos de inicio, como `.cshrc`, `.copy_files` y `.soffice` para todos los usuarios.	"Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 90
Iniciar sesión en modo a prueba de fallos.	Se corrigen los archivos de inicialización de usuario defectuosos.	"Cómo iniciar una sesión en modo a prueba de fallos en Trusted Extensions" en la página 93

▼ Cómo modificar atributos de etiquetas de usuarios predeterminados

Puede modificar los atributos de etiquetas de usuarios predeterminados durante la configuración del primer sistema. Los cambios se deben copiar en cada host de Trusted Extensions.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global. Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 53.

1 **Revise la configuración predeterminada de los atributos de usuario en el archivo `/etc/security/tsol/label_encodings`.**

Para conocer los valores predeterminados, consulte "Valores predeterminados del archivo `label_encodings`" en la página 80.

2 **Modifique la configuración de los atributos de usuario en el archivo `label_encodings`.**

Utilice el editor de confianza. Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57. En Trusted CDE, también puede

utilizar la acción Edit Label Encodings. Para obtener detalles, consulte "Cómo iniciar acciones administrativas de CDE en Trusted Extensions" en la página 56.

El archivo `label_encodings` debe ser el mismo en todos los hosts.

3 **Distribuya una copia del archivo en cada host de Trusted Extensions.**

▼ Cómo modificar los valores predeterminados de `policy.conf`

La modificación de los valores predeterminados de `policy.conf` en Trusted Extensions es similar a la modificación de cualquier archivo de sistema relativo a la seguridad en el SO Oracle Solaris. En Trusted Extensions, se utiliza un editor de confianza para modificar archivos de sistema.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global. Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 53.

1 **Revise los valores predeterminados en el archivo `/etc/security/policy.conf`.**

Para conocer las palabras clave de Trusted Extensions consulte la Tabla 6–1.

2 **Modifique la configuración.**

Utilice el editor de confianza para editar el archivo del sistema. Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

Ejemplo 7–1 Cambio de la configuración del tiempo de inactividad del sistema

En este ejemplo, el administrador de la seguridad desea que los sistemas inactivos regresen a la pantalla de inicio de sesión. El valor predeterminado bloquea los sistemas inactivos. Por lo tanto, el rol de administrador de la seguridad agrega el siguiente par palabra clave=valor `IDLECMD` al archivo `/etc/security/policy.conf`:

```
IDLECMD=LOGOUT
```

El administrador también desea que los sistemas permanezcan inactivos durante un período más corto antes de que se cierre la sesión. Por lo tanto, el rol de administrador de la seguridad agrega el siguiente par palabra clave=valor `IDLETIME` al archivo `policy.conf`:

```
IDLETIME=10
```

Así, el sistema cierra la sesión del usuario si el sistema permanece inactivo durante 10 minutos.

Ejemplo 7–2 Modificación del conjunto de privilegios básico de cada usuario

En este ejemplo, el administrador de la seguridad de una instalación de Sun Ray no quiere que los usuarios comunes vean los procesos de otros usuarios de Sun Ray. Por lo tanto, en todos los sistemas que estén configurados con Trusted Extensions, el administrador elimina `proc_info` desde el conjunto de privilegios básico. La configuración `PRIV_DEFAULT` del archivo `/etc/policy.conf` se modifica de la siguiente manera:

```
PRIV_DEFAULT=basic,!proc_info
```

Ejemplo 7–3 Asignación de las autorizaciones relacionadas con la impresión a todos los usuarios de un sistema

En este ejemplo, el administrador de la seguridad activa un equipo de un quiosco público para que imprima sin etiquetas si se escribe lo siguiente en el archivo del equipo `/etc/security/policy.conf`. La próxima vez que inicie, los trabajos de impresión de todos los usuarios de este quiosco se imprimen sin las etiquetas de las páginas.

```
AUTHS_GRANTED= solaris.print.unlabeled
```

A continuación, el administrador decide quitar las páginas de la carátula y del ubicador para ahorrar papel. Primero, se asegura de que la casilla Always Print Banners de Print Manager no esté seleccionada. Luego, modifica la entrada `policy.conf` para que se lea lo siguiente y reinicia. Así, todos los trabajos de impresión quedan sin etiquetas y no tienen las páginas de la carátula ni del ubicador.

```
AUTHS_GRANTED= solaris.print.unlabeled,solaris.print.nobanner
```

▼ Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions

Los usuarios pueden introducir los archivos `.copy_files` y `.link_files` en el directorio principal en la etiqueta que corresponde a la etiqueta de sensibilidad mínima. Los usuarios también pueden modificar los archivos `.copy_files` y `.link_files` que ya existen en la etiqueta mínima de los usuarios. Este procedimiento sirve para que el rol de administrador automatice la configuración del sitio.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global. Para obtener detalles, consulte "Cómo entrar en la zona global en Trusted Extensions" en la página 53.

1 Cree dos archivos de inicio de Trusted Extensions.

Agregará los archivos `.copy_files` y `.link_files` a la lista de archivos de inicio.

```
# cd /etc/skel
# touch .copy_files .link_files
```

2 Personalice el archivo `.copy_files`.

a. Inicie el editor de confianza.

Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

b. Escriba el nombre de ruta completo del archivo `.copy_files`.

```
/etc/skel/.copy_files
```

c. Escriba en `.copy_files`, uno por línea, los archivos que se copiarán en el directorio principal del usuario en todas las etiquetas.

Consulte "Archivos `.copy_files` y `.link_files`" en la página 84 para obtener ideas. Para ver archivos de muestra, consulte el Ejemplo 7–4.

3 Personalice el archivo `.link_files`.

a. Escriba el nombre de ruta completo del archivo `.link_files` en el editor de confianza.

```
/etc/skel/.link_files
```

b. Escriba en `.link_files`, uno por línea, los archivos que se enlazarán con el directorio principal del usuario en todas las etiquetas.

4 Personalice los otros archivos de inicio para sus usuarios.

- Para ver una explicación de lo que se debe incluir en los archivos de inicio, consulte "Personalización de un entorno de trabajo del usuario" de *Administración de Oracle Solaris: administración básica*.
- Para obtener detalles, consulte "Cómo personalizar los archivos de inicialización de usuario" de *Administración de Oracle Solaris: administración básica*.
- Si desea ver un ejemplo, consulte el Ejemplo 7–4.

5 (Opcional) Cree un subdirectorio `skelP` para los usuarios cuyo shell predeterminado sea un shell del perfil.

`P` indica el shell Profile.

6 Copie los archivos de inicio personalizados en el directorio de estructura básica apropiado.

7 Utilice el nombre de ruta `skel`*X* apropiado cuando cree el usuario.

X representa la letra con la que comienza el nombre del shell; por ejemplo, `B` para un shell Bourne, `K` para un shell Korn, `C` para un shell C y `P` para un shell Profile.

Ejemplo 7–4 Personalización de los archivos de inicio para los usuarios

En este ejemplo, el administrador de la seguridad configura archivos para el directorio principal de cada usuario. Los archivos se encuentran en su lugar antes de que cualquier usuario inicie sesión. Los archivos están en la etiqueta mínima del usuario. En este sitio, el shell predeterminado de los usuarios es el shell C.

El administrador de la seguridad crea un archivo `.copy_files` y un archivo `.link_files` en el editor de confianza que contengan lo siguiente:

```
## .copy_files for regular users
## Copy these files to my home directory in every zone
.mailrc
.mozilla
.soffice
:wq

## .link_files for regular users with C shells
## Link these files to my home directory in every zone
.cshrc
.login
.Xdefaults
.Xdefaults-hostname
:wq

## .link_files for regular users with Korn shells
# Link these files to my home directory in every zone
.ksh
.profile
.Xdefaults
.Xdefaults-hostname
:wq
```

En los archivos de inicialización del shell, el administrador garantiza que los trabajos de impresión de los usuarios se dirijan a una impresora con etiquetas.

```
## .cshrc file
setenv PRINTER conf-printer1
setenv LPDEST  conf-printer1

## .ksh file
export PRINTER conf-printer1
export LPDEST  conf-printer1
```

El administrador modifica el archivo `.Xdefaults-`*home-directory-server* para forzar el comando `dtterm` como origen del archivo `.profile` para un terminal nuevo.

```
## Xdefaults-HDserver
Dtterm*LoginShell: true
```

Los archivos personalizados se copian en el directorio de estructura básica apropiado.

```
$ cp .copy_files .link_files .cshrc .login .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelC
$ cp .copy_files .link_files .ksh .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelK
```

Errores más frecuentes Si crea archivos `.copy_files` en la etiqueta más baja y, a continuación, inicia sesión en una zona superior para ejecutar el comando `updatehome`, y el comando falla con un error de acceso, intente realizar lo siguiente:

- Verifique que desde la zona de nivel superior pueda ver el directorio de nivel inferior.

```
higher-level zone# ls /zone/lower-level-zone/home/username
ACCESS ERROR: there are no files under that directory
```

- Si no puede ver el directorio, reinicie el servicio de montaje automático en la zona de nivel superior:

```
higher-level zone# svcadm restart autofs
```

Salvo que use montajes de NFS para los directorios principales, el montador automático de la zona de nivel superior debe montar en bucle de retorno de `/zone/`*lower-level-zone*`/export/home/`*username* a `/zone/`*lower-level-zone*`/home/`*username*.

▼ Cómo iniciar una sesión en modo a prueba de fallos en Trusted Extensions

En Trusted Extensions, el inicio de sesión en modo a prueba de fallos está protegido. Si un usuario común personalizó los archivos de inicialización del shell y ahora no puede iniciar sesión, puede utilizar el inicio de sesión en modo a prueba de fallos para reparar los archivos del usuario.

Antes de empezar Debe conocer la contraseña `root`.

1 **Como en el SO Oracle Solaris, elija Options –> Failsafe Session en la pantalla de inicio de sesión.**

2 **Cuando aparezca el indicador, haga que el usuario proporcione el nombre de usuario y la contraseña.**

3 **En el indicador de la contraseña del usuario `root`, proporcione la contraseña para `root`.**

Ya puede depurar los archivos de inicialización del usuario.

Gestión de usuarios y derechos con Solaris Management Console (mapa de tareas)

En Trusted Extensions, debe utilizar Solaris Management Console para administrar los usuarios, las autorizaciones, los derechos y los roles. Para gestionar a los usuarios y sus atributos de seguridad, asuma el rol de administrador de la seguridad. El siguiente mapa de tareas describe las tareas comunes que debe realizar para los usuarios que operan en un entorno con etiquetas.

Tarea	Descripción	Para obtener instrucciones
Modificar el rango de etiquetas de un usuario.	Se modifican las etiquetas en las que el usuario puede trabajar. Es posible que las modificaciones restrinjan o amplíen el rango que el archivo `label_encodings` permite.	"Cómo modificar el rango de etiquetas de un usuario en Solaris Management Console" en la página 94
Crear un perfil de derechos para las autorizaciones convenientes.	Existen varias autorizaciones que pueden ser útiles para los usuarios comunes. Se crea un perfil para los usuarios que cumplen los requisitos para tener estas autorizaciones.	"Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 96
Modificar el conjunto de privilegios predeterminado del usuario.	Se elimina un privilegio del conjunto de privilegios predeterminado del usuario.	"Cómo restringir el conjunto de privilegios de un usuario" en la página 98
Impedir el bloqueo de cuentas para usuarios concretos.	Los usuarios que pueden asumir un rol deben tener desactivado el bloqueo de cuentas.	"Cómo impedir el bloqueo de cuentas de los usuarios" en la página 100
Permitir que un usuario vuelva a etiquetar datos.	Se autoriza a un usuario a reducir o aumentar el nivel de la información.	"Cómo activar a un usuario para que cambie el nivel de seguridad de los datos" en la página 100
Eliminar a un usuario del sistema.	Eliminar por completo a un usuario y sus procesos.	"Cómo suprimir una cuenta de usuario de un sistema Trusted Extensions" en la página 101
Manejar otras tareas.	Utilizar Solaris Management Console para manejar las tareas que no son específicas de Trusted Extensions.	"Manejo de otras tareas en Solaris Management Console (mapa de tareas)" en la página 102

▼ Cómo modificar el rango de etiquetas de un usuario en Solaris Management Console

Puede que desee ampliar el rango de etiquetas de un usuario para proporcionarle acceso de lectura a una aplicación administrativa. Por ejemplo, un usuario que puede iniciar sesión en la zona global, luego, podría ejecutar Solaris Management Console. El usuario podría ver los contenidos, pero no cambiarlos.

Como alternativa, es posible que desee restringir el rango de etiquetas del usuario. Por ejemplo, un usuario invitado puede estar limitado a una etiqueta.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Abra una caja de herramientas de Trusted Extensions en Solaris Management Console.**

   Utilice una caja de herramientas del ámbito adecuado. Para obtener detalles, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

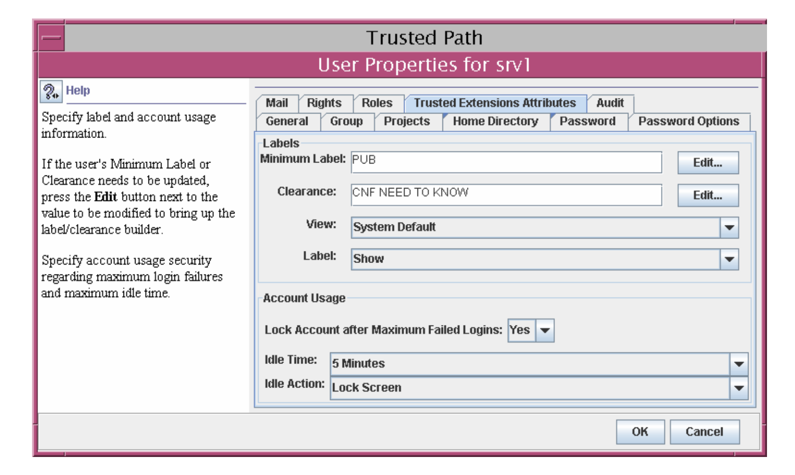
2. **En System Configuration, vaya a User Accounts.**

   Puede que se muestre el indicador de contraseña.

3. **Escriba la contraseña del rol.**

4. **Seleccione el usuario individual de User Accounts.**

5. **Haga clic en la ficha Trusted Extensions Attributes.**



   - **Para ampliar el rango de etiquetas del usuario, seleccione una acreditación superior.**

     También puede reducir la etiqueta mínima.

   - **Para restringir el rango de etiquetas a una etiqueta, haga la acreditación igual que la etiqueta mínima.**

6. **Para guardar los cambios, haga clic en OK.**

▼ Cómo crear perfiles de derechos para autorizaciones convenientes

Cuando la política de seguridad del sitio lo permita, quizás desee crear un perfil de derechos que contenga las autorizaciones para los usuarios que pueden realizar tareas que requieren autorización. Para activar a todos los usuarios de un sistema en particular que se van a autorizar, consulte "Cómo modificar los valores predeterminados de `policy.conf`" en la página 89.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Abra una caja de herramientas de Trusted Extensions en Solaris Management Console.**

   Utilice una caja de herramientas del ámbito adecuado. Para obtener detalles, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

2. **En System Configuration, vaya a Rights.**

   Puede que se muestre el indicador de contraseña.

3. **Escriba la contraseña del rol.**

4. **Para agregar un perfil de derechos, haga clic en Action –> Add Right.**

5. **Cree un perfil de derechos que contenga una o más de las siguientes autorizaciones.**

   Para conocer el procedimiento paso a paso, consulte "How to Create or Change a Rights Profile" de *System Administration Guide: Security Services*.

En la siguiente figura, la ventana Authorizations Included muestra las autorizaciones que pueden ser convenientes para los usuarios.

- Allocate Device: autoriza a un usuario para que asigne un dispositivo periférico, como un micrófono.

  De manera predeterminada, los usuarios de Oracle Solaris pueden leer y escribir en un CD-ROM. Sin embargo, en Trusted Extensions, solamente los usuarios que pueden asignar un dispositivo pueden acceder a la unidad de CD-ROM. Para asignar la unidad para su uso se requiere autorización. Por lo tanto, para leer y escribir en un CD-ROM en Trusted Extensions, los usuarios necesitan la autorización Allocate Device.
- Downgrade DragNDrop or CutPaste Info: autoriza a un usuario a seleccionar la información de un archivo de nivel superior y colocarla en un archivo de nivel inferior archivo.
- Downgrade File Label: autoriza a un usuario a disminuir el nivel de seguridad de un archivo
- DragNDrop or CutPaste without viewing contents: autoriza a un usuario a mover información sin que se vea la información que se mueve.
- Print Postscript: autoriza a un usuario a imprimir archivos PostScript.
- Print without Banner: autoriza a un usuario a que haga copias impresas sin la página de la carátula.
- Print without Label: autoriza a un usuario a que haga copias impresas que no muestren etiquetas.
- Remote Login: autoriza a un usuario a iniciar sesión de manera remota.
- Shutdown the System: autoriza a un usuario a cerrar el sistema y una zona.
- Upgrade DragNDrop or CutPaste Info: autoriza a un usuario a seleccionar información de un archivo de nivel inferior y colocarla en un archivo de nivel superior.
- Upgrade File Label: autoriza a un usuario a aumentar el nivel de seguridad de un archivo.

6 **Asigne el perfil de derechos a un usuario o a un rol.**

Si necesita asistencia, consulte la ayuda en pantalla. Para conocer el procedimiento paso a paso, consulte "How to Change the RBAC Properties of a User" de *System Administration Guide: Security Services*.

Ejemplo 7–5 Asignación de una autorización relacionada con la impresión a un rol

En el siguiente ejemplo, el administrador de la seguridad le permite a un rol imprimir los trabajos sin etiquetas en las páginas del cuerpo.

En Solaris Management Console, el administrador de la seguridad navega hasta Administrative Roles. El administrador ve los perfiles de derechos que se incluyen en un rol en particular y, luego, se asegura de que las autorizaciones relacionadas con la impresión se incluyan en uno de los perfiles de derechos del rol.

▼ Cómo restringir el conjunto de privilegios de un usuario

Puede que la seguridad del sitio requiera que a los usuarios se les otorgue menos privilegios que los asignados de manera predeterminada. Por ejemplo, en un sitio que utiliza Trusted Extensions en los sistemas Sun Ray, puede que desee impedir que los usuarios vean los procesos de los demás usuarios en el servidor Sun Ray.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 **Abra una caja de herramientas de Trusted Extensions en Solaris Management Console.**

Utilice una caja de herramientas del ámbito adecuado. Para obtener detalles, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

2 **En System Configuration, vaya a User Accounts.**

Puede que se muestre el indicador de contraseña.

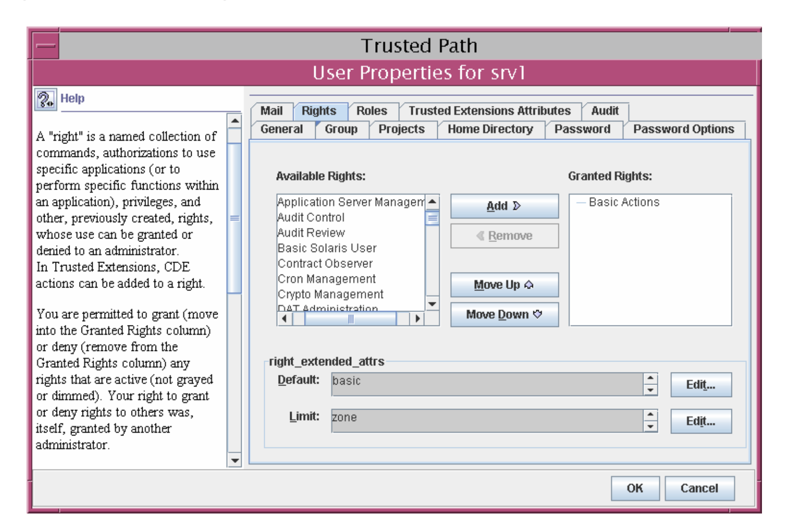
3 **Escriba la contraseña del rol.**

4 **Haga doble clic en el icono del usuario.**

5 **Elimine uno o varios de los privilegios del conjunto `basic`.**

a. **Haga doble clic en el icono del usuario.**

b. Haga clic en la ficha Rights.



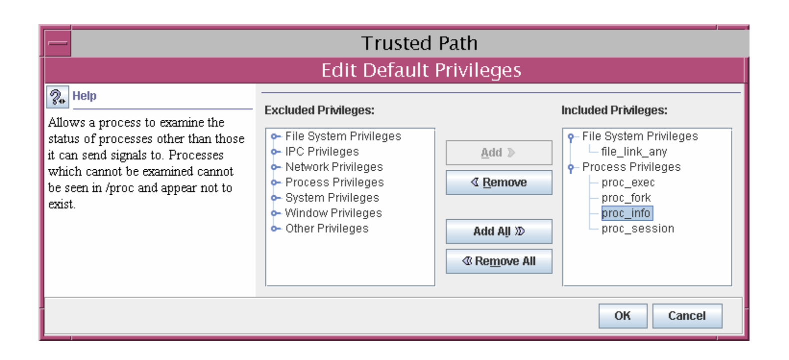
c. Haga clic en el botón Edit situado a la derecha del conjunto `basic` en el campo `right_extended_attr`.

d. Elimine `proc_session` o `file_link_any`.

Con la eliminación del privilegio `proc_session`, se impide que el usuario examine cualquier proceso que se encuentre fuera de su sesión actual. Con la eliminación del privilegio `file_link_any`, se impide que el usuario establezca enlaces físicos con archivos que no sean de su propiedad.



Precaución – No elimine los privilegios `proc_fork` o `proc_exec`. Sin estos privilegios, el usuario no podrá utilizar el sistema.



6 Para guardar los cambios, haga clic en OK.

▼ Cómo impedir el bloqueo de cuentas de los usuarios

Trusted Extensions amplía las funciones de seguridad del usuario en Solaris Management Console a fin de que se incluya el bloqueo de cuentas. Desactive el bloqueo de cuentas para los usuarios que pueden asumir un rol.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 Inicie Solaris Management Console.

Utilice una caja de herramientas del ámbito adecuado. Para obtener detalles, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

2 En System Configuration, vaya a User Accounts.

Puede que se muestre el indicador de contraseña.

3 Escriba la contraseña del rol.

4 Haga doble clic en el icono del usuario.

5 Haga clic en la ficha Trusted Extensions Attributes.

6 En la sección Account Usage, seleccione `No` del menú desplegable situado junto a `Lock account after maximum failed logins`.

7 Para guardar los cambios, haga clic en OK.

▼ Cómo activar a un usuario para que cambie el nivel de seguridad de los datos

Se puede autorizar a un usuario común o a un rol a cambiar el nivel de seguridad, o las etiquetas, de los archivos y los directorios. El usuario o el rol, además de tener la autorización, deben estar configurados para trabajar en más de una etiqueta. Las zonas con etiquetas deben estar configuradas de modo que se permita volver a etiquetar. Para conocer el procedimiento, consulte "Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas" en la página 139.



Precaución – El cambio del nivel de seguridad de los datos es una operación privilegiada. Esta tarea la deben realizar únicamente los usuarios de confianza.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Siga el procedimiento "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 96 para crear un perfil de derechos.**

   Las siguientes autorizaciones activan al usuario para que vuelva a etiquetar un archivo:

   - Downgrade File Label
   - Upgrade File Label

   Las siguientes autorizaciones activan al usuario para que vuelva a etiquetar la información de un archivo:

   - Downgrade DragNDrop or CutPaste Info
   - DragNDrop or CutPaste Info Without Viewing
   - Upgrade DragNDrop or CutPaste Info

2. **Utilice Solaris Management Console para asignar el perfil a los usuarios y los roles adecuados.**

   Si necesita asistencia, consulte la ayuda en pantalla. Para conocer el procedimiento paso a paso, consulte "How to Change the RBAC Properties of a User" de *System Administration Guide: Security Services*.

▼ Cómo suprimir una cuenta de usuario de un sistema Trusted Extensions

Cuando se elimina del sistema a un usuario, debe asegurarse de que también se supriman el directorio principal del usuario y cualquier otro objeto que sea propiedad del usuario. Como alternativa a la supresión de objetos que sean propiedad del usuario, puede transferir la propiedad de estos objetos a un usuario válido.

También debe asegurarse de que se supriman todos los trabajos por lotes que estén asociados con el usuario. Ningún objeto o proceso que pertenezca a un usuario eliminado puede permanecer en el sistema.

Antes de empezar Debe estar en el rol de administrador del sistema.

1. **Archive el directorio principal del usuario en cada etiqueta.**

2. **Archive los archivos de correo del usuario en cada etiqueta.**

3 En Solaris Management Console, suprima la cuenta del usuario.

a. Abra una caja de herramientas de Trusted Extensions en Solaris Management Console.

Utilice una caja de herramientas del ámbito adecuado. Para obtener detalles, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

b. En System Configuration, vaya a User Accounts.

Puede que se muestre el indicador de contraseña.

c. Escriba la contraseña del rol.

d. Seleccione la cuenta de usuario que desea eliminar y haga clic en el botón Delete.

Se le indicará que suprima el directorio principal del usuario y sus archivos de correo. Cuando acepta el indicador, el directorio principal del usuario y sus archivos de correo se suprimen solamente en la zona global.

4 En cada zona con etiquetas, suprima manualmente los directorios del usuario y sus archivos de correo.

Nota – Deberá buscar y suprimir los archivos temporales del usuario en todas las etiquetas, como los archivos de los directorios `/tmp`.

Manejo de otras tareas en Solaris Management Console (mapa de tareas)

Siga los procedimientos de Oracle Solaris para manejar las tareas en Solaris Management Console. Debe ser superusuario o estar en un rol de la zona global. El mapa de tareas siguiente hace referencia a las tareas básicas de Solaris Management Console.

Tarea	Para obtener instrucciones
Realizar tareas administrativas mediante Solaris Management Console.	Capítulo 2, "Trabajo con Solaris Management Console (tareas)" de *Administración de Oracle Solaris: administración básica*
Crear usuarios.	"Uso de las herramientas de gestión de Solaris con RBAC (mapa de tareas)" de *Administración de Oracle Solaris: administración básica*
Crear roles.	"How to Create and Assign a Role by Using the GUI" de *System Administration Guide: Security Services*

Tarea	Para obtener instrucciones
Modificar roles.	"How to Change the Properties of a Role" de *System Administration Guide: Security Services*
Crear o modificar un perfil de derechos.	"How to Create or Change a Rights Profile" de *System Administration Guide: Security Services*
Cambiar otros atributos de seguridad del usuario.	"How to Change the RBAC Properties of a User" de *System Administration Guide: Security Services*
Auditar las acciones de un rol.	"How to Audit Roles" de *System Administration Guide: Security Services*
Enumerar los perfiles de derechos con `smprofile list -D` *name-service-type*`:/`*server-name*`/`*domain-name*	*El Capítulo 9, "Using Role-Based Access Control (Tasks)" de System Administration Guide: Security Services* o la página del comando man `smprofile`(1M)



Administración remota en Trusted Extensions (tareas)

En este capítulo se describe cómo utilizar las herramientas administrativas de Trusted Extensions para administrar un sistema remoto.

Administración remota segura en Trusted Extensions

De manera predeterminada, Trusted Extensions no permite la administración remota. La administración remota implicaría un gran riesgo de seguridad si los usuarios de sistemas remotos que no son de confianza pudieran administrar los sistemas que están configurados con Trusted Extensions. Por esto, los sistemas se instalan inicialmente sin la opción que permite la administración de manera remota.

Hasta que la red se configura, todos los hosts remotos se asignan a la plantilla de seguridad `admin_low`. Por lo tanto, el protocolo CIPSO no se utiliza ni se acepta para ninguna conexión. En este estado inicial, los sistemas permanecen protegidos frente a los ataques remotos mediante varios mecanismos. Entre estos mecanismos, se incluyen la configuración de `netservices`, la política de inicio de sesión predeterminada y la política de módulos de autentificación enlazables (PAM, Plugable Authentication Modules).

- Cuando el perfil de la utilidad de gestión de servicio (SMF) `netservices` se establece como `limited`, no se activa ningún servicio remoto a excepción del shell seguro. Sin embargo, el servicio `ssh` no se puede utilizar para inicios de sesión remotos según lo establecido en las políticas de inicio de sesión y de PAM.
- La cuenta `root` no puede utilizarse para inicios de sesiones remotas porque la política predeterminada para `CONSOLE` en el archivo `/etc/default/login` impide que `root` inicie sesión de manera remota.
- Además, dos configuraciones de PAM afectan los inicios de sesión remotos.

El módulo pam_roles siempre rechaza los inicios de sesión locales desde las cuentas de tipo role. De manera predeterminada, este módulo también rechaza inicios de sesión remotos. Sin embargo, el sistema puede configurarse para que acepte los inicios de sesión remotos. Para ello, se debe especificar allow_remote en la entrada pam.conf del sistema.

Además, el módulo pam_tsol_account rechaza los inicios de sesión remotos en la zona global, salvo que se utilice el protocolo CIPSO. Esta política tiene por objeto que la administración remota se realice por medio de otro sistema Trusted Extensions.

Para activar la funcionalidad de inicio de sesión remoto, ambos sistemas deben asignar su igual a una plantilla de seguridad CIPSO. Si este enfoque no resulta práctico, se puede hacer que la política de protocolo de red sea menos estricta. Para ello, debe especificarse la opción allow_unlabeled en el archivo pam.conf. Si alguna de las políticas se hace menos estricta, la plantilla de red predeterminada debe cambiarse para que los equipos arbitrarios no puedan acceder a la zona global. La plantilla admin_low debe usarse con moderación, y la base de datos tnrhdb debe modificarse para que la dirección comodín 0.0.0.0 no se establezca como predeterminada para la etiqueta ADMIN_LOW. Para obtener detalles, consulte "Administración remota de Trusted Extensions (mapa de tareas)" en la página 108 y "Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 192.

Métodos para administrar sistemas remotos en Trusted Extensions

Normalmente, los administradores utilizan los comandos rlogin y ssh para administrar sistemas remotos desde la línea de comandos. También se puede utilizar Solaris Management Console. En Trusted CDE, el programa dtappsession puede iniciar acciones de Trusted CDE de manera remota. A partir de la versión Solaris 10 5/09, se puede utilizar un equipo de red virtual (VNC, Virtual Networking Computer) para mostrar de forma remota un escritorio de varios niveles.

Los siguientes métodos de administración remota son posibles en Trusted Extensions:

- Un usuario root puede iniciar sesión en un host remoto desde un terminal. Consulte "Cómo iniciar sesión de manera remota desde la línea de comandos en Trusted Extensions" en la página 109. Este método funciona como en el sistema Oracle Solaris. Este método resulta inseguro.
- Un rol puede iniciar sesión en un host remoto desde un terminal en el espacio de trabajo del rol. Consulte "Cómo iniciar sesión de manera remota desde la línea de comandos en Trusted Extensions" en la página 109.
- Los administradores pueden iniciar un servidor Solaris Management Console que se esté ejecutando en un sistema remoto. Consulte "Cómo administrar sistemas de manera remota con Solaris Management Console desde un sistema Trusted Extensions" en la página 111.

- Las acciones de la carpeta Trusted_Extensions pueden iniciarse de manera remota mediante el comando `dtappsession`. Consulte "Cómo administrar Trusted Extensions con `dtappsession` de manera remota" en la página 110.
- El usuario puede iniciar sesión en un escritorio de varios niveles que sea remoto mediante un programa de cliente vnc para conectarse al servidor Xvnc en un sistema Trusted Extensions. Consulte "Cómo utilizar Xvnc para acceder de manera remota a un sistema Trusted Extensions" en la página 115.

Inicio de sesión remoto por un rol en Trusted Extensions

Como en el SO Oracle Solaris, se debe cambiar una configuración en el archivo `/etc/default/login` de cada host para permitir inicios de sesión remotos. Además, puede que sea necesario modificar el archivo `pam.conf`. En Trusted Extensions, el administrador de la seguridad es el responsable del cambio. Para conocer los procedimientos, consulte "Enable Remote Login by root User in Trusted Extensions" de *Trusted Extensions Configuration Guide* y "Enable Remote Login by a Role in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

En los hosts de Trusted Extensions y Oracle Solaris, los inicios de sesión remotos pueden requerir autorización o pueden no requerirla. "Gestión de inicio de sesión remoto en Trusted Extensions" en la página 108 describe las condiciones y los tipos de inicios de sesión que requieren autorización. De manera predeterminada, los roles tienen la autorización Remote Login.

Administración remota basada en roles desde hosts sin etiquetas

En Trusted Extensions, los usuarios asumen roles mediante el menú Trusted Path. Los roles operan en espacios de trabajo de confianza. De manera predeterminada, los roles no pueden asumirse fuera de Trusted Path. Si la política del sitio lo permite, el administrador de la seguridad puede cambiar la política predeterminada. Los administradores de hosts sin etiquetas que ejecuten el software de cliente de Solaris Management Console 2.1 pueden administrar los hosts de confianza.

- Para cambiar la política predeterminada, consulte "Enable Remote Login by a Role in Trusted Extensions" de *Trusted Extensions Configuration Guide*.
- Para administrar sistemas de manera remota, consulte "Cómo iniciar sesión de manera remota desde la línea de comandos en Trusted Extensions" en la página 109.

Este cambio de política se aplica solamente cuando el usuario del sistema remoto sin etiquetas tiene una cuenta de usuario en el host de Trusted Extensions. El usuario de Trusted Extensions debe tener la capacidad para asumir un rol administrativo. El rol puede usar Solaris Management Console para administrar el sistema remoto.



Precaución – Si se activa la administración remota desde un host que no es de Trusted Extensions, el entorno administrativo queda menos protegido que un espacio de trabajo administrativo de Trusted Extensions. Tenga cuidado al escribir contraseñas y otros datos confidenciales. Como medida de precaución, cierre todas las aplicaciones que no sean de confianza antes de iniciar Solaris Management Console.

Gestión de inicio de sesión remoto en Trusted Extensions

El inicio de sesión remoto entre dos hosts de Trusted Extensions se considera una extensión de la sesión actual.

No se requiere autorización cuando el comando `rlogin` no solicita una contraseña. Si un archivo `/etc/hosts.equiv` o un archivo `.rhosts` del directorio principal del usuario en el host remoto muestra el nombre de usuario o el host desde el que se intenta efectuar el inicio de sesión remoto, no se requiere contraseña. Para obtener más información, consulte las páginas del comando man `rhosts(4)` y `rlogin(1)`.

Para todos los demás inicios de sesión remotos, incluidos los inicios de sesión con el comando `ftp`, se requiere la autorización Remote Login.

Para crear un perfil de derechos que incluya la autorización Remote Login, consulte "Gestión de usuarios y derechos con Solaris Management Console (mapa de tareas)" en la página 94.

Administración remota de Trusted Extensions (mapa de tareas)

En el siguiente mapa de tareas se describen las tareas que se utilizan para administrar un sistema Trusted Extensions remoto.

Tarea	Descripción	Para obtener instrucciones
Activar al usuario `root` para que inicie sesión de manera remota en un sistema Trusted Extensions.	Activar al usuario `root` para que trabaje de manera remota desde un sistema con etiquetas.	"Enable Remote Login by root User in Trusted Extensions" de *Trusted Extensions Configuration Guide*
Activar un rol para que inicie sesión de manera remota en un sistema Trusted Extensions.	Permitir que cualquier rol a trabaje de manera remota desde un sistema con etiquetas.	"Enable Remote Login by a Role in Trusted Extensions" de *Trusted Extensions Configuration Guide*

Tarea	Descripción	Para obtener instrucciones
Activar el inicio de sesión remoto desde un sistema sin etiquetas en un sistema Trusted Extensions.	Permitir que cualquier usuario o rol a trabaje de manera remota desde un sistema sin etiquetas.	"Enable Remote Login From an Unlabeled System" de *Trusted Extensions Configuration Guide*
Iniciar sesión de manera remota en un sistema Trusted Extensions.	Iniciar sesión como rol en un sistema Trusted Extensions.	"Cómo iniciar sesión de manera remota desde la línea de comandos en Trusted Extensions" en la página 109
Administrar un sistema de manera remota.	Utilizar el comando `dtappsession` para administrar el sistema remoto con acciones de Trusted_Extensions.	"Cómo administrar Trusted Extensions con `dtappsession` de manera remota" en la página 110
	Utilizar Solaris Management Console para administrar el host remoto desde un sistema Trusted Extensions.	"Cómo administrar sistemas de manera remota con Solaris Management Console desde un sistema Trusted Extensions" en la página 111
	Utilizar Solaris Management Console para administrar hosts de Trusted Extensions remotos desde un sistema sin etiquetas.	"Cómo administrar sistemas de manera remota con Solaris Management Console desde un sistema sin etiquetas" en la página 113
Administrar y utilizar un sistema remoto.	Utilizar el servidor Xvnc en el sistema Trusted Extensions remoto para mostrar al cliente una sesión de varios niveles desde cualquier cliente.	"Cómo utilizar Xvnc para acceder de manera remota a un sistema Trusted Extensions" en la página 115
Activar a usuarios específicos para que inicien sesión en la zona global.	Utilizar las herramientas de red y usuarios de Solaris Management Console para activar a usuarios específicos a que accedan a la zona global.	"Cómo activar a usuarios específicos para que inicien sesión de manera remota en la zona global en Trusted Extensions" en la página 115

▼ Cómo iniciar sesión de manera remota desde la línea de comandos en Trusted Extensions

---

Nota – El comando `telnet` no puede utilizarse para la asunción de roles remota porque no puede transferir la identidad principal y las identidades de roles al módulo `pam_roles`.

Antes de empezar El usuario y el rol deben estar definidos de manera idéntica en el sistema local y en el sistema remoto.

El rol debe tener la autorización Remote Login. De manera predeterminada, esta autorización se encuentra en los perfiles de derechos de administración remota y mantenimiento y reparación.

El administrador de la seguridad debe haber completado el procedimiento "Enable Remote Login by a Role in Trusted Extensions" de *Trusted Extensions Configuration Guide* en cada sistema que pueda administrarse de manera remota. Si el sistema puede administrarse desde un sistema sin etiquetas, significa que el procedimiento de "Enable Remote Login From an Unlabeled System" de *Trusted Extensions Configuration Guide* también se ha completado.

- **Desde el espacio de trabajo de un usuario que puede asumir un rol, inicie sesión en el host remoto.**

  Utilice los comandos `rlogin`, `ssh` o `ftp`.

  - Si los comandos `rlogin -l` o `ssh` se utilizan para iniciar sesión, todos los comandos de los perfiles de derechos del rol se encuentran disponibles.
  - Si se utiliza el comando `ftp`, consulte la página del comando man `ftp(1)` para conocer los comandos disponibles.

▼ Cómo administrar Trusted Extensions con `dtappsession` de manera remota

El programa `dtappsession` activa a un administrador para que administre un sistema remoto que ejecuta CDE.

`dtappsession` es útil cuando un sistema remoto no tiene supervisor. Por ejemplo, `dtappsession` se usa con frecuencia para administrar dominios en servidores grandes. Para obtener más información, consulte la página del comando man `dtappsession(1)`.

Antes de empezar En un sistema con etiquetas, debe estar en un rol administrativo en la zona global. En un sistema sin etiquetas, debe asumir un rol que esté definido en el sistema remoto. A continuación, debe ejecutar el inicio de sesión remoto desde el shell del perfil del rol.

1. **(Opcional) Cree un espacio de trabajo que esté dedicado a la sesión remota.**

   A fin de evitar confusiones entre las aplicaciones de CDE remotas y cualquier aplicación local, dedique espacio de trabajo de un rol administrativo para este procedimiento. Para obtener detalles, consulte "How to Add a Workspace at a Particular Label" de *Trusted Extensions User's Guide*.

2. **Inicie sesión en el host remoto.**

   Puede utilizar los comandos `rlogin` o `ssh`.

   ```
   $ ssh remote-host
   ```

3 **Inicie la administración remota.**

En la ventana de terminal de la sesión, escriba el comando `dtappsession` seguido del nombre del host local.

```
$ /usr/dt/bin/dtappsession local-host
```

Si Application Manager se está ejecutando en el host remoto, se muestra en el host local. Además, aparece un cuadro de diálogo de salida.

4 **Administre el host remoto.**

Si invocó la sesión remota desde Trusted CDE, puede utilizar acciones en la carpeta Trusted_Extensions.

5 **Cuando termine, haga clic en el botón Exit.**





Precaución – No se recomienda cerrar Application Manager; esto no finaliza la sesión.

6 **En la ventana de terminal, salga de la sesión remota.**

Además, utilice el comando `hostname` para verificar que está en el host local.

```
$ exit
$ hostname
local-host
```

Cómo administrar sistemas de manera remota con Solaris Management Console desde un sistema Trusted Extensions

Solaris Management Console ofrece una interfaz de administración remota para gestionar los usuarios, los derechos, los roles y la red. Debe asumir un rol para usar la consola. En este procedimiento, ejecute la consola en el sistema local y especifique el sistema remoto como servidor.

Antes de empezar Debe haber completado los siguientes procedimientos:

- En ambos sistemas: "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*
- En el sistema remoto: "Enable Remote Login by a Role in Trusted Extensions" de *Trusted Extensions Configuration Guide* y "Enable the Solaris Management Console to Accept Network Communications" de *Trusted Extensions Configuration Guide*
- En el sistema remoto que es el servidor LDAP: "Configuring the Solaris Management Console for LDAP (Task Map)" de *Trusted Extensions Configuration Guide*

1 **En el sistema local, inicie sesión como el usuario que se define de manera idéntica en el sistema remoto.**

2 **Asuma el rol que desea utilizar para administrar el sistema.**

3 **En el rol, inicie Solaris Management Console.**

Para obtener detalles, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

a. **En el cuadro de diálogo del servidor, escriba el nombre del servidor remoto.**

- **Si está utilizando LDAP como un servicio de nombres, escriba el nombre del servidor LDAP.**

  A continuación, seleccione uno de los siguientes ámbitos.

  - **Para administrar las bases de datos del servicio de nombres, seleccione la caja de herramientas `Scope=LDAP`.**

    `This Computer (`*ldap-server*`: Scope=LDAP, Policy=TSOL)`

  - **Para administrar los archivos locales en el servidor LDAP, seleccione la caja de herramientas `Scope=Files`.**

    `This Computer (`*ldap-server*`: Scope=Files, Policy=TSOL)`

- **Si no utiliza LDAP como servicio de nombres, escriba el nombre del sistema remoto que desea administrar.**

  A continuación, seleccione la caja de herramientas `Scope=Files`.

  `This Computer (`*remote-system*`: Scope=Files, Policy=TSOL)`

4 **Seleccione una herramienta en System Configuration.**

Al seleccionar una herramienta como User, aparece un cuadro de diálogo con el nombre del servidor de Solaris Management Console, el nombre de usuario, el nombre de rol y un espacio para escribir la contraseña del rol. Asegúrese de que las entradas sean correctas.

5 **Con el rol que está definido de manera idéntica en los sistemas locales y remotos, inicie sesión en el servidor de Solaris Management Console.**

Escriba la contraseña del rol y haga clic en Login as Role. A continuación, puede utilizar Solaris Management Console para administrar el sistema.

Nota – Aunque puede utilizar Solaris Management Console para ejecutar `dtappsession`, la manera más sencilla de usar `dtappsession` se describe en "Cómo administrar Trusted Extensions con `dtappsession` de manera remota" en la página 110.

▼ Cómo administrar sistemas de manera remota con Solaris Management Console desde un sistema sin etiquetas

En este procedimiento, se ejecutan el cliente y el servidor de Solaris Management Console en el sistema remoto, y se muestra la consola en el sistema local.

Antes de empezar El sistema Trusted Extensions debe tener asignada la etiqueta `ADMIN_LOW` en el sistema local.

Nota – El sistema que no ejecuta el protocolo CIPSO, como el sistema Trusted Solaris, es un sistema sin etiquetas desde la perspectiva de un sistema Trusted Extensions.

El servidor de Solaris Management Console en el sistema remoto debe estar configurado para aceptar la conexión remota. Para conocer el procedimiento, consulte "Enable the Solaris Management Console to Accept Network Communications" de *Trusted Extensions Configuration Guide*.

Los dos sistemas deben tener el mismo usuario que tiene asignado el mismo rol que puede utilizar Solaris Management Console. El usuario puede tener el rango de etiquetas del usuario común, pero el rol debe tener el rango de `ADMIN_LOW` a `ADMIN_HIGH`.

Debe estar en un rol administrativo de la zona global.

1 **Active el servidor X local para que muestre la consola Solaris Management Console remota.**

```
# xhost + TX-SMC-Server
# echo $DISPLAY
:n.n
```

2 **En el sistema local, debe emplear un usuario que pueda asumir un rol para Solaris Management Console.**

```
# su - same-username-on-both-systems
```

3 Con ese usuario, inicie sesión en el servidor remoto como el rol.

```
$ rlogin -l same-rolename-on-both-systems  TX-SMC-Server
```

4 Asegúrese de que las variables del entorno que Solaris Management Console utiliza tengan los valores correctos.

a. Establezca el valor de la variable `DISPLAY`.

```
$ DISPLAY=local:n.n
$ export DISPLAY=local:n.n
```

b. Establezca el valor de la variable `LOGNAME` para el nombre de usuario.

```
$ LOGNAME=same-username-on-both-systems
$ export LOGNAME=same-username-on-both-systems
```

c. Establezca el valor de la variable `USER` para el nombre del rol.

```
$ USER=same-rolename-on-both-systems
$ export USER=same-rolename-on-both-systems
```

5 En el rol, inicie Solaris Management Console desde la línea de comandos.

```
$ /usr/sbin/smc &
```

6 Seleccione una herramienta en System Configuration.

Al seleccionar una herramienta como User, aparece un cuadro de diálogo con el nombre del servidor de Solaris Management Console, el nombre de usuario, el nombre de rol y un espacio para escribir la contraseña del rol. Asegúrese de que las entradas sean correctas.

7 Como rol, inicie sesión en el servidor.

Escriba la contraseña del rol y haga clic en Login as Role. A continuación, puede utilizar Solaris Management Console para administrar el sistema.

Nota – Si intenta acceder a la información de la base de datos de la red desde un sistema distinto del servidor LDAP, la operación fallará. La consola le permite iniciar sesión en el host remoto y abrir la caja de herramientas. Sin embargo, si intenta acceder a la información o modificarla, el siguiente mensaje de error le indicará que ha seleccionado `Scope=LDAP` en un sistema distinto del servidor LDAP:

```
Management server cannot perform the operation requested.
...
Error extracting the value-from-tool.
The keys received from the client were machine, domain, Scope.
Problem with Scope.
```

▼ Cómo activar a usuarios específicos para que inicien sesión de manera remota en la zona global en Trusted Extensions

El rango de etiquetas predeterminado del usuario y el comportamiento predeterminado de la zona se cambian a fin de activar a quienes no tengan roles para que inicien sesión de manera remota. Quizás desee llevar a cabo este procedimiento para un evaluador que utiliza un sistema con etiquetas remoto. Por motivos de seguridad, el sistema del evaluador debe ejecutar una etiqueta separada de los demás usuarios.

Antes de empezar Debe tener una muy buena razón para permitir que el usuario inicie sesión en la zona global.

Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Si desea activar a usuarios específicos para que inicien sesión en la zona global, asígneles un rango de etiquetas administrativas.**

   Utilice Solaris Management Console para asignar una acreditación de `ADMIN_HIGH` y una etiqueta mínima de `ADMIN_LOW` a cada usuario. Para obtener detalles, consulte "Cómo modificar el rango de etiquetas de un usuario en Solaris Management Console" en la página 94.

   Las zonas con etiquetas del usuario también deben permitir el inicio de sesión.

2. **Para activar el inicio de sesión remoto desde una zona con etiquetas en la zona global, realice lo siguiente.**

   a. **Agregue un puerto de varios niveles para el inicio de sesión remoto en la zona global.**

   Utilice Solaris Management Console. El puerto 513 mediante el protocolo TCP activa el inicio de sesión remoto. Para ver un ejemplo, consulte "Cómo crear un puerto de varios niveles para una zona" en la página 141.

   b. **Lea los cambios de `tnzonecfg` en el núcleo.**

   ```
   # tnctl -fz /etc/security/tsol/tnzonecfg
   ```

   c. **Reinicie el servicio de inicio de sesión remoto.**

   ```
   # svcadm restart svc:/network/login:rlogin
   ```

▼ Cómo utilizar Xvnc para acceder de manera remota a un sistema Trusted Extensions

La tecnología de informática en red virtual (VNC) conecta un cliente a un servidor remoto y, luego, muestra el escritorio del servidor remoto en una ventana en el cliente. Xvnc es la versión

UNIX de VNC, que se basa en un servidor X estándar. En Trusted Extensions, un cliente de cualquier plataforma puede conectarse a una Xvnc que ejecute el software de Trusted Extensions e iniciar sesión en el servidor Xvnc para visualizar un escritorio de varios niveles y trabajar en él.

Antes de empezar Debe tener instalado y configurado el software de Trusted Extensions en el sistema que se va a utilizar como servidor Xvnc. Debe haber creado e iniciado las zonas con etiquetas. El servidor Xvnc reconoce los clientes VNC por nombre de host o dirección IP.

Debe ser superusuario en la zona global del sistema que se utilizará como servidor Xvnc.

1 Configure el servidor Xvnc.

Para obtener más información, consulte las páginas del comando man `Xvnc(1)` y `vncconfig(1)`.



Precaución – Si ejecuta las versiones Solaris 10 10/08 o Solaris 10 5/08, debe aplicar los parches en el sistema antes de configurar el servidor. En el sistema SPARC, instale la versión más reciente del parche 125719. En el sistema x86, instale la versión más reciente del parche 125720.

---

a. Cree el directorio de configuración Xservers.

```
# mkdir -p /etc/dt/config
```

b. Copie el archivo `/usr/dt/config/Xservers` en el directorio `/etc/dt/config`.

```
# cp /usr/dt/config/Xservers /etc/dt/config/Xservers
```

c. Edite el archivo `/etc/dt/config/Xservers` para iniciar el programa Xvnc en lugar de Xserver o Xorg.

En este ejemplo, la entrada está configurada para iniciar sesión en el servidor sin contraseña. Para iniciar la sesión el escritorio de manera correcta, el UID local debe ser `none` en lugar de `console`.

La entrada se divide con fines de visualización. La entrada debe ocupar solamente una línea.

```
#   :0  Local local_uid@console root /usr/X11/bin/Xserver :0 -nobanner
  :0  Local local_uid@none root /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024x768x24 -depth 24
```

Nota – Para que la configuración sea más segura, se debe solicitar una contraseña mediante el parámetro `-SecurityTypes VncAuth`. La página del comando man `Xvnc(1)` describe los requisitos de las contraseñas.

---

d. Reinicie el servidor o inicie el servidor Xvnc.

```
# reboot
```

Después de reiniciar, verifique que el programa Xvnc se esté ejecutando.

```
# ps -ef | grep Xvnc
  root  2145  932  0  Jan 18 ?  6:15 /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024
```

2 En cada cliente VNC del servidor Xvnc de Trusted Extensions, instale el software del cliente VNC.

Para el sistema cliente, puede elegir el software. En este ejemplo se utiliza el software para VNC de Sun.

```
# cd SUNW-pkg-directory
# pkgadd -d . SUNWvncviewer
```

3 En una ventana de terminal de un cliente VNC, conéctese al servidor.

```
% /usr/bin/vncviewer Xvnc-server-hostname
```

4 En la ventana que aparece, escriba su nombre y contraseña.

Continúe con el proceso de inicio de sesión. Para obtener una descripción del resto de los pasos, consulte "Logging In to Trusted Extensions" de *Trusted Extensions User's Guide*.

Si inició sesión en el servidor como superusuario, puede administrar el servidor de manera inmediata. Si inició sesión en el servidor como usuario, debe asumir un rol para administrar el sistema.



Trusted Extensions y LDAP (descripción general)

En este capítulo se describe el uso de Oracle Directory Server Enterprise Edition (servidor de directorios) para sistemas que estén configurados con Trusted Extensions.

Uso del servicio de nombres en Trusted Extensions

Para alcanzar una uniformidad entre el usuario, el host y los atributos de red dentro de un dominio de seguridad con varios sistemas Trusted Extensions, se usa un servicio de nombres para distribuir la mayor parte de la información de configuración. LDAP es un ejemplo de un servicio de nombres. El archivo `nsswitch.conf` determina qué servicio de nombres se utiliza. LDAP es el servicio de nombres recomendado para Trusted Extensions.

El servidor de directorios puede proporcionar el servicio de nombres LDAP para los clientes de Trusted Extensions y Oracle Solaris. El servidor debe incluir bases de datos de red de Trusted Extensions, y los clientes de Trusted Extensions deben conectarse al servidor mediante un puerto de varios niveles. El administrador de la seguridad especifica el puerto de varios niveles cuando configura Trusted Extensions.

Trusted Extensions agrega dos bases de datos de red de confianza al servidor LDAP: `tnrhdb` y `tnrhtp`. Estas bases se administran mediante la herramienta Security Templates de Solaris Management Console. Una caja de herramientas de `Scope=LDAP, Policy=TSOL` almacena los cambios de configuración en el servidor de directorios.

- Para obtener información sobre el uso del servicio de nombres LDAP en el SO Oracle Solaris, consulte la *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*.
- La configuración de los clientes del servidor de directorios para Trusted Extensions se describen en la *Trusted Extensions Configuration Guide* . Los sistemas Trusted Extensions pueden ser clientes de un servidor LDAP de Oracle Solaris mediante un servidor proxy LDAP que esté configurado con Trusted Extensions.

Nota – Los sistemas que se configuran con Trusted Extensions no pueden ser clientes de servidores maestros NIS o NIS+.

Sistemas Trusted Extensions que no están en red

Si un servicio de nombres no se usa en un sitio, los administradores deben asegurarse de que la información de configuración para los usuarios, los hosts y las redes sea idéntica en todos los hosts. Si se realiza un cambio en un host, dicho cambio debe aplicarse también en todos los demás hosts.

En un sistema Trusted Extensions que no está en red, la información de configuración se mantiene en los directorios `/etc`, `/etc/security` y `/etc/security/tsol`. Las acciones de la carpeta Trusted_Extensions le permiten modificar algunas partes de la información de configuración. La herramienta Security Templates de Solaris Management Console le permite modificar los parámetros de la base de datos de red. Los usuarios, los roles y los derechos se modifican mediante las herramientas User Accounts, Administrative Roles y Rights. Una caja de herramientas en This Computer con `Scope=Files, Policy=TSOL` almacena localmente los cambios de configuración.

Bases de datos LDAP de Trusted Extensions

Trusted Extensions amplía el esquema del servidor de directorios para acomodar las bases de datos `tnrhdb` y `tnrhtp`. Trusted Extensions define dos atributos nuevos, `ipTnetNumber` y `ipTnetTemplateName`, y dos clases de objeto nuevas, `ipTnetTemplate` y `ipTnetHost`.

Los atributos se definen de la siguiente manera:

```
ipTnetNumber
   ( 1.3.6.1.1.1.1.34 NAME 'ipTnetNumber'
     DESC 'Trusted network host or subnet address'
```

```
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )

ipTnetTemplateName
   ( 1.3.6.1.1.1.1.35 NAME 'ipTnetTemplateName'
     DESC 'Trusted network template name'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )
```

Las clases de objeto se definen de la siguiente manera:

```
ipTnetTemplate
   ( 1.3.6.1.1.1.2.18 NAME 'ipTnetTemplate' SUP top STRUCTURAL
     DESC 'Object class for Trusted network host templates'
     MUST ( ipTnetTemplateName )
     MAY ( SolarisAttrKeyValue ) )

ipTnetHost
   ( 1.3.6.1.1.1.2.19 NAME 'ipTnetHost' SUP top AUXILIARY
     DESC 'Object class for Trusted network host/subnet address
           to template mapping'
     MUST ( ipTnetNumber $ ipTnetTemplateName ) )
```

La plantilla de definición `cipso` en LDAP es similar a la siguiente:

```
ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=organizationalUnit
 ou=ipTnet

 ipTnetTemplateName=cipso,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 ipTnetTemplateName=cipso
 SolarisAttrKeyValue=host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;

 ipTnetNumber=0.0.0.0,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 objectClass=ipTnetHost
 ipTnetNumber=0.0.0.0
 ipTnetTemplateName=internal
```

Uso del servicio de nombres LDAP en Trusted Extensions

El servicio de nombres LDAP se gestiona en Trusted Extensions, como en el SO Oracle Solaris. A continuación, se proporcionan algunos comandos útiles con referencias para obtener información más detallada:

- Para conocer estrategias de resolución de problemas de configuración LDAP, consulte el Capítulo 13, "LDAP Troubleshooting (Reference)" de *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.
- Para resolver problemas de conexión entre clientes y servidores LDAP que se ven afectados por etiquetas, consulte "Cómo depurar una conexión de cliente con el servidor LDAP" en la página 206.
- Para resolver otros problemas de conexión entre clientes y servidores LDAP, consulte el Capítulo 13, "LDAP Troubleshooting (Reference)" de *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.
- Para visualizar las entradas LDAP desde un cliente LDAP, escriba:

```
$ ldaplist -l
$ ldap_cachemgr -g
```

- Para visualizar las entradas LDAP desde un servidor LDAP, escriba:

```
$ ldap_cachemgr -g
$ idsconfig -v
```

- Para visualizar los hosts que LDAP gestiona, escriba:

```
$ ldaplist -l hosts       Long listing
$ ldaplist hosts       One-line listing
```

- Para crear una lista con la información del árbol de información de directorios (DIT, Directory Information Tree) en LDAP, escriba:

```
$ ldaplist -l services | more
dn: cn=apocd+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
  objectClass: ipService
  objectClass: top
  cn: apocd
  ipServicePort: 38900
  ipServiceProtocol: udp

...
$ ldaplist services name
dn=cn=name+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
```

- Para visualizar el estado del servicio LDAP en el cliente, escriba:

```
# svcs -xv network/ldap/client
svc:/network/ldap/client:default (LDAP client)
 State: online since date
   See: man -M /usr/share/man -s 1M ldap_cachemgr
   See: /var/svc/log/network-ldap-client:default.log
Impact: None.
```

- Para iniciar o detener el cliente LDAP, escriba:

```
# svcadm enable network/ldap/client
```

```
# svcadm disable network/ldap/client
```

- Para iniciar o detener el servidor LDAP en la versión 5.2 del software de Oracle Directory Server Enterprise Edition, escriba:

```
# installation-directory/slap-LDAP-server-hostname/start-slapd
# installation-directory/slap-LDAP-server-hostname/stop-slapd
```

- Para iniciar o detener el servidor LDAP en la versión 6 del software de Oracle Directory Server Enterprise Edition, escriba:

```
# dsadm start /export/home/ds/instances/your-instance
# dsadm stop /export/home/ds/instances/your-instance
```

- Para iniciar o detener un servidor proxy LDAP en la versión 6 del software de Oracle Directory Server Enterprise Edition, escriba:

```
# dpadm start /export/home/ds/instances/your-instance
# dpadm stop /export/home/ds/instances/your-instance
```

CAPÍTULO 10

Gestión de zonas en Trusted Extensions (tareas)

En este capítulo se describe cómo funcionan las zonas no globales en los sistemas que están configurados con Trusted Extensions. Además, se explican procedimientos exclusivos de las zonas en Trusted Extensions.

Zonas en Trusted Extensions

El sistema Trusted Extensions bien configurado consta de una zona global, que es la instancia del sistema operativo, y una o más zonas no globales con etiquetas. Durante la configuración, Trusted Extensions anexa una sola etiqueta a cada zona; lo que crea las zonas con etiquetas. Las etiquetas proceden del archivo `label_encodings`. Los administradores pueden crear una zona para cada una de las etiquetas, pero esto no es obligatorio. Es posible tener más etiquetas que zonas con etiquetas en un sistema. No es posible tener más zonas con etiquetas que etiquetas.

Por lo general, en el sistema Trusted Extensions, los sistemas de archivos de una zona suelen montarse en bucle de retorno como sistemas de archivos de bucle de retorno (LOFS, Loopback File System). Todos los archivos y directorios que se pueden escribir en una zona con etiquetas se encuentran en la etiqueta de la zona. De manera predeterminada, el usuario puede visualizar los archivos que están en una zona de una etiqueta inferior a la etiqueta actual del usuario. Esta configuración permite a los usuarios ver sus directorios principales en las etiquetas inferiores a la etiqueta del espacio de trabajo actual. Aunque los usuarios pueden ver los archivos en una etiqueta inferior, no pueden modificarlos. Los usuarios pueden modificar solamente los archivos de un proceso que tenga la misma etiqueta que el archivo.

En Trusted Extensions, la zona global es una zona administrativa. Las zonas con etiquetas son para los usuarios comunes. Los usuarios pueden trabajar en una zona cuya etiqueta se encuentre dentro del rango de acreditación del usuario.

Cada zona tiene una dirección IP asociada y atributos de seguridad. Las zonas pueden configurarse con puertos de varios niveles (MLP, Multilevel Ports). Asimismo, las zonas se pueden configurar con una política para la difusión del protocolo de mensajes de control de Internet (ICMP, Internet Control Message Protocol), como `ping`.

Para obtener información sobre cómo compartir directorios desde una zona con etiquetas y sobre el montaje de directorios desde zonas con etiquetas de manera remota, consulte el Capítulo 11, "Gestión y montaje de archivos en Trusted Extensions (tareas)".

Las zonas de Trusted Extensions, están integradas en el producto de zonas de Oracle Solaris. Para obtener detalles, consulte la Parte II, "Zones" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*. En particular, los problemas de instalación de parches y paquetes afectan Trusted Extensions. Para obtener detalles, consulte el Capítulo 25, "About Packages and Patches on an Oracle Solaris System With Zones Installed (Overview)" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones* y el Capítulo 30, "Troubleshooting Miscellaneous Oracle Solaris Zones Problems" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

Zonas y direcciones IP en Trusted Extensions

El equipo de configuración inicial asignó direcciones IP a la zona global y a las zonas con etiquetas. En "Creating Labeled Zones" de *Trusted Extensions Configuration Guide*, se documentan tres tipos de configuraciones:

- El sistema tiene una dirección IP para la zona global y todas las zonas con etiquetas.

  Esta configuración es útil para los sistemas que utilizan software de DHCP para obtener su dirección IP. Si no se espera que ningún usuario inicie sesión, el servidor LDAP puede tener esta configuración.
- El sistema tiene una dirección IP para la zona global y otra dirección IP que comparten todas las zonas, incluida la zona global. Cualquier zona puede tener una combinación de una dirección exclusiva y una dirección compartida.

  Esta configuración es útil para los sistemas en que los usuarios comunes iniciarán sesión. También se puede utilizar para una impresora o un servidor NFS. Esta configuración conserva las direcciones IP.
- El sistema tiene una dirección IP para la zona global, y cada zona con etiquetas tiene una dirección IP exclusiva.

  Esta configuración sirve para proporcionar acceso a redes físicas separadas de sistemas de un solo nivel. Normalmente, cada zona tiene una dirección IP en una red física diferente de las demás zonas con etiquetas. Debido a que esta configuración se implementa con una sola instancia de IP, la zona global controla las interfaces físicas y gestiona los recursos globales, como la tabla de enrutamiento.

Con la introducción de las instancias de IP exclusivas para las zonas no globales, se suma un cuarto tipo de configuración al SO Oracle Solaris. A partir de la versión Solaris 10 8/07, se pueden asignar instancias de IP propias a las zonas no globales y se pueden gestionar las interfaces físicas propias de estas zonas. En esta configuración, cada zona opera como si fuera un sistema distinto. Para obtener una descripción, consulte "Zone Network Interfaces" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

Sin embargo, en una configuración de este tipo, cada zona con etiquetas opera como si fuera un sistema de una sola etiqueta distinto. Las funciones de redes de varios niveles de Trusted Extensions se basan en las funciones de una pila de IP compartida. Los procedimientos de administración en Trusted Extensions asumen que la zona global controla las redes por completo. Por lo tanto, si el equipo de configuración inicial instaló zonas con etiquetas con instancias de IP exclusivas, debe proporcionar o consultar documentación específica del sitio.

Zonas y puertos de varios niveles

De manera predeterminada, las zonas no pueden enviar paquetes a ninguna otra zona ni recibir paquetes de ninguna otra zona. Los puertos de varios niveles activan servicios concretos en un puerto para aceptar solicitudes dentro de un rango de etiquetas o de un conjunto de etiquetas. Estos servicios con privilegios pueden responder en la etiqueta de la solicitud. Por ejemplo, quizás desee crear un puerto de explorador web con privilegios que pueda recibir todas las etiquetas, pero cuyas respuestas estén restringidas por etiqueta. De manera predeterminada, las zonas con etiquetas no tienen puertos de varios niveles.

El rango o el conjunto de etiquetas que restringe los paquetes que el puerto de varios niveles puede aceptar se basan en la dirección IP de la zona. Se asigna a la dirección IP una plantilla de host remoto en la base de datos `tnrhdb`. El rango o el conjunto de etiquetas en la plantilla del host remoto restringen los paquetes que el puerto de varios niveles puede aceptar.

- Las restricciones en los puertos de varios niveles para las configuraciones de direcciones IP diferentes son las siguientes:
- En los sistemas en que la zona global tiene una dirección IP y cada zona con etiquetas tiene una sola dirección IP, se puede agregar un puerto de varios niveles para un servicio en particular a cada zona. Por ejemplo, el sistema podría configurarse para que el servicio `ssh`, mediante el puerto TCP 22, sea un puerto de varios niveles en la zona global y en cada zona con etiquetas.
- En una configuración típica, a la zona global se le asigna una dirección IP, y las zonas con etiquetas comparten una segunda dirección IP con la zona global. Cuando se agrega un puerto de varios niveles a una interfaz compartida, el paquete de servicio se enruta hacia la zona con etiquetas donde se define el puerto de varios niveles. El paquete se acepta únicamente si la plantilla del host remoto para la zona con etiquetas incluye la etiqueta del paquete. Si el rango es `ADMIN_LOW` a `ADMIN_HIGH`, se aceptan todos los paquetes. Si el rango fuera menor, se descartarían los paquetes que no estén dentro del rango.

En la mayoría de los casos, una zona puede definir un puerto determinado para que actúe como puerto de varios niveles en una interfaz compartida. En la situación anterior, donde el puerto `ssh` está configurado como puerto de varios niveles compartido en una zona no global, ninguna otra zona puede recibir conexiones `ssh` en la dirección compartida. Sin embargo, la zona global podría definir el puerto `ssh` como puerto de varios niveles privado para la recepción de conexiones en su dirección específica de la zona.

- En un sistema en el que la zona global y las zonas con etiquetas comparten una dirección IP, se podría agregar un puerto de varios niveles para el servicio `ssh` a una zona. Si el puerto de varios niveles para `ssh` se agrega a la zona global, ninguna zona con etiquetas puede agregar un puerto de varios niveles para el servicio `ssh`. De manera similar, si el puerto de varios niveles para el servicio `ssh` se agrega a una zona con etiquetas, la zona global no se puede configurar con un puerto de varios niveles `ssh`.

Para ver un ejemplo de la agregación de puertos de varios niveles a las zonas con etiquetas, consulte el Ejemplo 13–16.

Zonas e ICMP en Trusted Extensions

Las redes transmiten mensajes de difusión y envían paquetes de ICMP a los sistemas de la red. En un sistema de varios niveles, estas transmisiones pueden colapsar el sistema en cada etiqueta. De manera predeterminada, la política de red para las zonas con etiquetas requiere que los paquetes de ICMP se reciban únicamente en la etiqueta que coincide.

Procesos de la zona global y de las zonas con etiquetas

En Trusted Extensions, la política de MAC se aplica a todos los procesos, incluso los procesos de la zona global. Los procesos de la zona global se ejecutan en la etiqueta `ADMIN_HIGH`. Cuando se comparten los archivos de una zona global, se comparten en la etiqueta `ADMIN_LOW`. Por lo tanto, dado que MAC impide que un proceso con una etiqueta superior modifique un objeto de nivel inferior, generalmente la zona global no puede escribir en un sistema montado en NFS.

Sin embargo, en un número limitado de los casos, las acciones en una zona con etiquetas puede requerir que un proceso de la zona global modifique un archivo en dicha zona.

A fin de activar un proceso de la zona global para que monte un sistema de archivos remoto con permisos de lectura y escritura, el montaje debe estar en la ruta de la zona cuya etiqueta corresponde a la del sistema de archivos remoto. El montaje no debe estar en la ruta root de la zona.

- El sistema de montaje debe tener una zona en la etiqueta idéntica como el sistema de archivos remoto.
- El sistema debe montar el sistema de archivos remoto en la ruta de la zona que tiene etiquetas idénticas.

El sistema *no* debe montar el sistema de archivos remoto en la *ruta root de la zona* de la zona que tiene etiquetas idénticas.

Tenga en cuenta una zona que esté denominada como `public` en la etiqueta `PUBLIC`. La *ruta de la zona* es `/zone/public/`. Todos los directorios de la ruta de la zona se encuentran en la etiqueta `PUBLIC`; por ejemplo:

```
/zone/public/dev
/zone/public/etc
/zone/public/home/username
/zone/public/root
/zone/public/usr
```

De los directorios de la ruta de la zona, solamente los archivos que se encuentran en `/zone/public/root` son visibles desde la zona public. A los demás directorios y archivos en la etiqueta `PUBLIC` se puede acceder solamente desde la zona global. La ruta `/zone/public/root` es la *ruta raíz de la zona*.

Desde la perspectiva del administrador de la zona public, la ruta root de la zona se ve como `/`. De manera similar, el administrador de la zona public no puede acceder a un directorio principal del usuario en la ruta de la zona (directorio `/zone/public/home/`*username*). Dicho directorio se ve solamente desde la zona global. La zona public monta ese directorio en la ruta root de la zona como `/home/`*username*. Desde la perspectiva de la zona global, este montaje se ve como `/zone/public/root/home/`*username*.

El administrador de la zona public puede modificar `/home/`*username*. Cuando los archivos del directorio principal del usuario deben modificarse, el proceso de la zona global no utiliza dicha ruta. La zona global utiliza el directorio principal del usuario en la ruta de la zona, `/zone/public/home/`*username*.

- Los archivos y directorios que se encuentran en la ruta de la zona, `/zone/`*zonename*`/`, pero no en la ruta raíz de la zona, directorio `/zone/`*zonename*`/root` , pueden modificarse mediante un proceso de la zona global que se ejecute en la etiqueta `ADMIN_HIGH`.
- El administrador de la zona con etiquetas puede modificar los archivos y directorios de la ruta root de la zona, `/zone/public/root`.

Por ejemplo, cuando un usuario asigna un dispositivo en la zona public, un proceso de la zona global que se ejecuta en la etiqueta `ADMIN_HIGH` modifica el directorio `dev` en la ruta de la zona, `/zone/public/dev`. De manera similar, cuando un usuario guarda una configuración del escritorio, un proceso de la zona global de `/zone/public/home/`*username* modifica el archivo de la configuración del escritorio. Por último, para compartir archivos desde una zona con etiquetas, el administrador de la zona global crea el archivo de configuración, `dfstab`, en la ruta de la zona, `/zone/public/etc/dfs/dfstab`. El administrador de la zona con etiquetas no puede acceder a ese archivo y no puede compartir archivos desde la zona con etiquetas. Para obtener información sobre cómo compartir un directorio con etiquetas, consulte "Cómo compartir directorios desde una zona con etiquetas" en la página 153.

Utilidades de administración de zonas en Trusted Extensions

Algunas tareas de administración de la zona pueden realizarse desde la línea de comandos. Sin embargo, la manera más sencilla de administrar la zona consiste en utilizar las interfaces gráficas de usuario que Trusted Extensions proporciona:

- Los atributos de seguridad de la configuración de la zona se llevan a cabo con la herramienta Trusted Network Zones de Solaris Management Console. Para obtener una descripción de esta herramienta, consulte "Herramienta Trusted Network Zones" en la página 41. Para ver ejemplos de configuración y creación de la zona, consulte el Capítulo 4, "Configuring Trusted Extensions (Tasks)" de *Trusted Extensions Configuration Guide* y "Cómo crear un puerto de varios niveles para una zona" en la página 141.
- La secuencia de comandos del shell, `/usr/sbin/txzonemgr`, proporciona un asistente basado en menú para crear, instalar, inicializar e iniciar zonas. Si está administrando las zonas desde Solaris Trusted Extensions (JDS), utilice la secuencia de comandos `txzonemgr` en lugar de las acciones de Trusted CDE. `txzonemgr` utiliza el comando `zenity`. Para obtener detalles, consulte la página del comando man `zenity`(1).
- En Trusted CDE, la configuración y la creación de zonas se puede llevar a cabo con acciones en la carpeta Trusted_Extensions. Para obtener una descripción de las acciones, consulte "Acciones de Trusted CDE" en la página 35. Para conocer los procedimientos que utilizan las acciones, consulte "Cómo iniciar acciones administrativas de CDE en Trusted Extensions" en la página 56.

Gestión de zonas (mapa de tareas)

El mapa de tareas siguiente describe las tareas de gestión de zonas que son específicas de Trusted Extensions. El mapa también hace referencia a los procedimientos comunes que se realizan en Trusted Extensions de la misma manera en que se realizan en un sistema de Oracle Solaris.

Tarea	Descripción	Para obtener instrucciones
Ver todas las zonas.	En cualquier etiqueta, se visualizan las zonas dominadas por la zona actual.	"Cómo visualizar las zonas que están preparadas o en ejecución" en la página 132
Ver directorios montados.	En cualquier etiqueta, se visualizan los directorios dominados por la etiqueta actual.	"Cómo visualizar las etiquetas de los archivos montados" en la página 133
Permitir que los usuarios comunes vean un archivo `/etc`.	Se monta en bucle de retorno un directorio o archivo de la zona global que no es visible de manera predeterminada en una zona con etiquetas.	"Cómo montar en bucle de retorno un archivo que no suele estar visible en una zona con etiquetas" en la página 134

Tarea	Descripción	Para obtener instrucciones
Impedir que los usuarios comunes visualicen un directorio principal de nivel inferior desde una etiqueta de nivel superior.	De manera predeterminada, los directorios de nivel inferior son visibles desde las zonas de nivel superior. Cuando desactiva el montaje de una zona de nivel inferior, puede desactivar todos los montajes de las zonas de nivel inferior.	“Cómo desactivar el montaje de archivos de nivel inferior” en la página 135
Configurar una zona para permitir el cambio de las etiquetas en los archivos.	Las zonas con etiquetas tienen privilegios limitados. De manera predeterminada, las zonas con etiquetas no tienen el privilegio que permite que un usuario autorizado vuelva a etiquetar un archivo. Se debe modificar la configuración de zona para agregar el privilegio.	“Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas” en la página 139
Poner un archivo o directorio en una zona con etiquetas o sacarlo de ella.	Cambiar el nivel de seguridad de un archivo o directorio mediante el cambio de su etiqueta.	“How to Move Files Between Labels in Trusted CDE” de *Trusted Extensions User's Guide*
Anexar un conjunto de datos ZFS a una zona con etiquetas y compartirlo.	Se monta un conjunto de datos ZFS con permisos de lectura y escritura en una zona con etiquetas y se comparte la parte de sólo lectura del conjunto de datos con una zona superior.	“Cómo compartir un conjunto de datos ZFS desde una zona con etiquetas” en la página 137.
Configurar una zona nueva.	Se crea una zona en una etiqueta que no se esté utilizando actualmente para etiquetar una zona en este sistema.	Consulte “Name and Label the Zone” de *Trusted Extensions Configuration Guide*. Luego, siga el procedimiento que el equipo de configuración inicial utilizó para crear las otras zonas. Consulte “Creating Labeled Zones” de *Trusted Extensions Configuration Guide* para obtener información paso a paso.
Crear un puerto de varios niveles para una aplicación.	Los puertos de varios niveles son útiles para los programas que requieren un avance de varios niveles en una zona con etiquetas.	“Cómo configurar un puerto de varios niveles para NFSv3 mediante `udp`” en la página 141 “Cómo crear un puerto de varios niveles para una zona” en la página 141
Resolver problemas de acceso y montaje NFS.	Se depuran los problemas de acceso generales para los montajes y, quizás, para las zonas.	“Cómo resolver problemas por fallos de montaje en Trusted Extensions” en la página 160
Eliminar una zona con etiquetas.	Se elimina por completo una zona con etiquetas del sistema.	“How to Remove a Non-Global Zone” de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*

▼ Cómo visualizar las zonas que están preparadas o en ejecución

Este procedimiento crea una secuencia de comandos de shell que muestra las etiquetas de la zona actual y de todas las zonas dominadas por la zona actual.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1. **Utilice el editor de confianza para crear la secuencia de comandos `getzonelabels`.**

   Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

   Proporcione el nombre de la ruta de la secuencia de comandos; por ejemplo, `/usr/local/scripts/getzonelabels`.

2. **Agregue el siguiente contenido y guarde el archivo:**

```
#!/bin/sh
#
echo "NAME\t\tSTATUS\t\tLABEL"
echo "====\t\t======\t\t====="
myzone=‘zonename‘
for i in ‘/usr/sbin/zoneadm list -p‘ ; do
        zone=‘echo $i | cut -d ":" -f2‘
        status=‘echo $i | cut -d ":" -f3‘
        path=‘echo $i | cut -d ":" -f4‘
        if [ $zone != global ]; then
                if [ $myzone = global ]; then
                        path=$path/root/tmp
                else
                        path=$path/export/home
                fi
        fi
        label=‘/usr/bin/getlabel -s $path |cut -d ":" -f2-9‘
        if [ ‘echo $zone|wc -m‘ -lt 8 ]; then
                echo "$zone\t\t$status\t$label"
        else
                echo "$zone\t$status\t$label"
        fi
done
```

3. **Pruebe la secuencia de comandos en la zona global.**

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
global          running         ADMIN_HIGH
needtoknow      running         CONFIDENTIAL : NEED TO KNOW
restricted      ready           CONFIDENTIAL : RESTRICTED
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

Cuando la secuencia de comandos se ejecuta desde la zona global, se muestran las etiquetas de todas las zonas que están preparadas o en ejecución. Aquí está la salida de la zona global para las zonas que se crearon a partir del archivo `label_encodings` predeterminado:

Ejemplo 10–1 Visualización de las etiquetas de todas las zonas preparadas o en ejecución

En el siguiente ejemplo, un usuario ejecuta la secuencia de comandos `getzonelabels` en la zona `internal`.

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

▼ Cómo visualizar las etiquetas de los archivos montados

Este procedimiento crea una secuencia de comandos de shell que muestra los sistemas de archivos montados de la zona actual. Cuando la secuencia de comandos se ejecuta desde la zona global, muestra las etiquetas de todos los sistemas de archivos montados en cada zona.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1. **Utilice el editor de confianza para crear la secuencia de comandos `getmounts`.**

   Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

   Proporcione el nombre de la ruta de la secuencia de comandos; por ejemplo, `/usr/local/scripts/getmounts`.

2. **Agregue el siguiente contenido y guarde el archivo:**

```
#!/bin/sh
#
for i in ‘/usr/sbin/mount -p | cut -d " " -f3‘ ; do
        /usr/bin/getlabel $i
done
```

3. **Pruebe la secuencia de comandos en la zona global.**

```
# /usr/local/scripts/getmounts
/:      ADMIN_LOW
/dev:   ADMIN_LOW
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
```

```
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/zone/restricted/export/home:   CONFIDENTIAL : RESTRICTED
/proc:  ADMIN_LOW
/system/contract:       ADMIN_LOW
/etc/svc/volatile:      ADMIN_LOW
/etc/mnttab:    ADMIN_LOW
/dev/fd:        ADMIN_LOW
/tmp:           ADMIN_LOW
/var/run:       ADMIN_LOW
/zone/public/export/home:  PUBLIC
/root:          ADMIN_LOW
```

Ejemplo 10–2 Visualización de las etiquetas de los sistemas de archivos en la zona restricted

Cuando un usuario común ejecuta la secuencia de comandos desde una zona con etiquetas, la secuencia de comandos `getmounts` muestra las etiquetas de todos los sistemas de archivos montados en dicha zona. En un sistema en el que las zonas se crean para cada etiqueta en el archivo `label_encodings` predeterminado, la salida de la zona `restricted` es la siguiente:

```
# /usr/local/scripts/getmounts
/:      CONFIDENTIAL : RESTRICTED
/dev:   CONFIDENTIAL : RESTRICTED
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/proc:  CONFIDENTIAL : RESTRICTED
/system/contract:       CONFIDENTIAL : RESTRICTED
/etc/svc/volatile:      CONFIDENTIAL : RESTRICTED
/etc/mnttab:    CONFIDENTIAL : RESTRICTED
/dev/fd:        CONFIDENTIAL : RESTRICTED
/tmp:   CONFIDENTIAL : RESTRICTED
/var/run:       CONFIDENTIAL : RESTRICTED
/zone/public/export/home:       PUBLIC
/home/gfaden:   CONFIDENTIAL : RESTRICTED
```

▼ Cómo montar en bucle de retorno un archivo que no suele estar visible en una zona con etiquetas

Este procedimiento activa a un usuario en una zona con etiquetas especificada para que vea los archivos que no se exportaron desde la zona global de manera predeterminada.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1 **Detenga la zona cuya configuración desea cambiar.**

```
# zoneadm -z zone-name halt
```

2 **Monte en bucle de retorno un archivo o directorio.**

Por ejemplo, permita que los usuarios comunes vean un archivo en el directorio `/etc`.

```
# zonecfg -z zone-name
 add filesystem
 set special=/etc/filename
 set directory=/etc/filename
 set type=lofs
 add options [ro,nodevices,nosetuid]
 end
 exit
```

Nota – Hay algunos archivos que el sistema no utiliza, por lo que montarlos en bucle de retorno no causaría ningún efecto. Por ejemplo, el software de Trusted Extensions no comprueba el archivo `/etc/dfs/dfstab` en una zona con etiquetas. Para obtener más información, consulte "Uso compartido de archivos desde una zona con etiquetas" en la página 147.

---

3 **Inicie la zona.**

```
# zoneadm -z zone-name boot
```

Ejemplo 10–3 Montaje en bucle de retorno del archivo `/etc/passwd`

En este ejemplo, el administrador de la seguridad desea permitir que los evaluadores y los programadores verifiquen si sus contraseñas locales se encuentran establecidas. Después de que se detiene la zona `sandbox`, esta se configura para montar en bucle de retorno el archivo `passwd`. A continuación, la zona se reinicia.

```
# zoneadm -z sandbox halt
# zonecfg -z sandbox
 add filesystem
    set special=/etc/passwd
    set directory=/etc/passwd
    set type=lofs
    add options [ro,nodevices,nosetuid]
 end
 exit
# zoneadm -z sandbox boot
```

▼ Cómo desactivar el montaje de archivos de nivel inferior

De manera predeterminada, los usuarios pueden ver los archivos de nivel inferior. Eliminar el privilegio `net_mac_aware` para impedir la visualización de todos los archivos de nivel inferior de una zona en particular. Para obtener una descripción del privilegio `net_mac_aware`, consulte la página del comando man `privileges(5)`.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1. **Detenga la zona cuya configuración desea cambiar.**

```
# zoneadm -z zone-name halt
```

2. **Configure la zona para impedir la visualización de los archivos de nivel inferior.**

   Elimine el privilegio `net_mac_aware` de la zona.

```
# zonecfg -z zone-name
 set limitpriv=default,!net_mac_aware
 exit
```

3. **Reinicie la zona.**

```
# zoneadm -z zone-name boot
```

Ejemplo 10–4 Cómo impedir que los usuarios vean los archivos de nivel inferior

En este ejemplo, el administrador de la seguridad desea impedir que los usuarios en un sistema se confundan. Por lo tanto, los usuarios pueden ver únicamente los archivos de la etiqueta en la que están trabajando. Entonces, el administrador de la seguridad impide la visualización de todos los archivos de nivel inferior. En este sistema, los usuarios no pueden ver los archivos que se encuentran disponibles públicamente, a menos que estén trabajando en la etiqueta `PUBLIC`. Además, los usuarios sólo pueden montar archivos en NFS en la etiqueta de las zonas.

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z restricted boot

# zoneadm -z needtoknow halt
# zonecfg -z needtoknow
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z needtoknow boot

# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z internal boot
```

Dado que `PUBLIC` es la etiqueta mínima, el administrador de la seguridad no ejecuta los comandos para la zona `PUBLIC`.

▼ Cómo compartir un conjunto de datos ZFS desde una zona con etiquetas

En este procedimiento, monta un conjunto de datos ZFS con permisos de lectura y escritura en una zona con etiquetas. Ya que todos los comandos se ejecutan en la zona global, el administrador de la zona global controla la agregación de conjuntos de datos ZFS a las zonas con etiquetas.

Como mínimo, la zona con etiquetas debe estar en el estado `ready` para compartir un conjunto de datos. La zona puede estar en el estado `running`.

Antes de empezar Para configurar la zona con el conjunto de datos, primero debe detener la zona.

1. **Cree el conjunto de datos ZFS.**

```
# zfs create datasetdir/subdir
```

El nombre del conjunto de datos puede incluir un directorio, como `zone/data`.

2. **En la zona global, detenga la zona con etiquetas.**

```
# zoneadm -z labeled-zone-name halt
```

3. **Defina el punto de montaje del conjunto de datos.**

```
# zfs set mountpoint=legacy datasetdir/subdir
```

La configuración de la propiedad ZFS `mountpoint` establece la etiqueta del punto de montaje cuando el punto de montaje corresponde a una zona con etiquetas.

4. **Agregue el conjunto de datos a la zona como un sistema de archivos.**

```
# zonecfg -z labeled-zone-name
# zonecfg:labeled-zone-name> add fs
# zonecfg:labeled-zone-name:dataset> set dir=/subdir
# zonecfg:labeled-zone-name:dataset> set special=datasetdir/subdir
# zonecfg:labeled-zone-name:dataset> set type=zfs
# zonecfg:labeled-zone-name:dataset> end
# zonecfg:labeled-zone-name> exit
```

Si se agrega el conjunto de datos como un sistema de archivos, el conjunto de datos se monta en `/data` en la zona, antes de que se interprete el archivo `dfstab`. Este paso garantiza que el conjunto de datos no se monte antes de que se inicie la zona. En concreto, se inicia la zona, se monta el conjunto de datos y, luego, se interpreta el archivo `dfstab`.

5. **Comparta el conjunto de datos.**

Agregue una entrada para el sistema de archivos del conjunto de datos al archivo `/zone/`*labeled-zone-name*`/etc/dfs/dfstab`. Esta entrada también utiliza el nombre de ruta `/`*subdir*.

```
share  -F nfs  -d "dataset-comment"  /subdir
```

6 Inicie la zona con etiquetas.

zoneadm -z *labeled-zone-name* **boot**

Cuando se inicia la zona, se monta el conjunto de datos automáticamente como punto de montaje de lectura y escritura en la zona *labeled-zone-name* con la etiqueta de la zona *labeled-zone-name*.

Ejemplo 10–5 Uso compartido y montaje de un conjunto de datos ZFS desde zonas con etiquetas

En este ejemplo, el administrador agrega un conjunto de datos de ZFS a la zona `needtoknow` y, luego, lo comparte. El conjunto de datos, `zone/data`, se encuentra asignado al punto de montaje `/mnt`. Los usuarios de la zona `restricted` pueden ver el conjunto de datos.

En primer lugar, el administrador detiene la zona.

```
# zoneadm -z needtoknow halt
```

Dado que el conjunto de datos se encuentra asignado a un punto de montaje diferente, el administrador elimina la asignación anterior y, a continuación, establece el nuevo punto de montaje.

```
# zfs set zoned=off zone/data
# zfs set mountpoint=legacy zone/data
```

A continuación, en la interfaz interactiva `zonecfg`, el administrador agrega explícitamente el conjunto de datos a la zona `needtoknow`.

```
# zonecfg -z needtoknow
# zonecfg:needtoknow> add fs
# zonecfg:needtoknow:dataset> set dir=/data
# zonecfg:needtoknow:dataset> set special=zone/data
# zonecfg:needtoknow:dataset> set type=zfs
# zonecfg:needtoknow:dataset> end
# zonecfg:needtoknow> exit
```

A continuación, el administrador modifica el archivo `/zone/needtoknow/etc/dfs/dfstab` para compartir el conjunto de datos. Luego, inicia la zona `needtoknow`.

```
## Global zone dfstab file for needtoknow zone
share  -F nfs  -d "App Data on ZFS"  /data
```

```
# zoneadm -z needtoknow boot
```

Finalmente se podrá acceder al conjunto de datos.

Los usuarios de la zona `restricted`, que domina la zona `needtoknow`, pueden ver el conjunto de datos montado. Para ello, deben cambiar al directorio `/data`. Deben usar la ruta completa para acceder al conjunto de datos montado desde la perspectiva de la zona global. En este ejemplo, `machine1` es el nombre de host del sistema que incluye la zona con etiquetas. El administrador asignó este nombre de host a una dirección IP no compartida.

```
# cd /net/machine1/zone/needtoknow/root/data
```

Errores más frecuentes Si el intento de acceder al conjunto de datos desde la etiqueta superior devuelve los mensajes de error `not found` o `No such file or directory`, el administrador debe reiniciar el servicio del montador automático mediante la ejecución del comando `svcadm restart autofs`.

▼ Cómo permitir que los archivos se vuelvan a etiquetar desde una zona con etiquetas

Este procedimiento es un requisito previo para que un usuario pueda volver a etiquetar archivos.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 **Detenga la zona cuya configuración desea cambiar.**

```
# zoneadm -z zone-name halt
```

2 **Configure la zona para activar la opción de volver a etiquetar.**

Agregue los privilegios adecuados a la zona. Los privilegios de las ventanas permiten a los usuarios emplear las operaciones arrastrar y soltar, y cortar y pegar.

- **Para activar las disminuciones de niveles, agregue el privilegio `file_downgrade_sl` a la zona.**

```
# zonecfg -z zone-name
 set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
 win_mac_write,win_selection,file_downgrade_sl
 exit
```

- **Para activar las actualizaciones, agregue a la zona los privilegios `sys_trans_label` y `file_upgrade_sl`.**

```
# zonecfg -z zone-name
 set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
 win_mac_write,win_selection,sys_trans_label,file_upgrade_sl
 exit
```

- **Para activar los aumentos o las disminuciones de niveles, agregue los tres privilegios a la zona.**

```
# zonecfg -z zone-name
 set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
 win_mac_write,win_selection,sys_trans_label,file_downgrade_sl,
 file_upgrade_sl
 exit
```

3 **Reinicie la zona.**

```
# zoneadm -z zone-name boot
```

Para conocer los requisitos del proceso y del usuario que permiten volver a etiquetar, consulte la página del comando man `setflabel`(3TSOL). Para saber cómo autorizar a un usuario a que vuelva a etiquetar archivos, consulte "Cómo activar a un usuario para que cambie el nivel de seguridad de los datos" en la página 100.

Ejemplo 10–6 Activación de aumentos de nivel desde la zona internal

En este ejemplo, el administrador de la seguridad desea activar a los usuarios autorizados de un sistema para que puedan aumentar el nivel de los archivos. Cuando el administrador activa a los usuarios a aumentar el nivel de la información, les permite proteger la información con el mayor nivel de seguridad. En la zona global, el administrador ejecuta los siguientes comandos de administración de la zona.

```
# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,sys_trans_label,file_upgrade_sl
 exit
# zoneadm -z internal boot
```

Así, los usuarios autorizados pueden aumentar el nivel de la información de `internal` a `restricted` desde la zona `internal`.

Ejemplo 10–7 Activación de disminuciones de nivel desde la zona restricted

En este ejemplo, el administrador de la seguridad desea activar a los usuarios autorizados de un sistema para que puedan disminuir el nivel de los archivos. Debido a que el administrador no agrega privilegios de las ventanas a la zona, los usuarios autorizados no pueden utilizar File Manager para volver a etiquetar archivos. Para volver a etiquetar archivos, los usuarios deben utilizar el comando `setlabel`.

Cuando el administrador activa a los usuarios a disminuir el nivel de la información, permite que los usuarios de menor nivel de seguridad puedan acceder a los archivos. En la zona global, el administrador ejecuta los siguientes comandos de administración de la zona.

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,file_downgrade_sl
 exit
# zoneadm -z restricted boot
```

Así, los usuarios autorizados pueden disminuir el nivel de la información de `restricted` a `internal` o `public` desde la zona `restricted` con el comando `setlabel`.

▼ Cómo configurar un puerto de varios niveles para NFSv3 mediante udp

Este procedimiento se utiliza para activar los montajes de lectura en sentido descendente para NFSv3 mediante `udp`. Para agregar el puerto de varios niveles se utiliza Solaris Management Console.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Inicie Solaris Management Console.**

   Para obtener detalles, consulte "Cómo administrar el sistema local con Solaris Management Console" en la página 55.

2. **Seleccione la caja de herramientas Files.**

   El título de la caja de herramientas incluye `Scope=Files, Policy=TSOL`.

3. **Configure la zona y el puerto de varios niveles.**

   a. **Vaya a la herramienta Trusted Network Zones.**

   b. **Haga doble clic en la zona global.**

   c. **Agregue un puerto de varios niveles para el protocolo UDP:**

      i. **Haga clic en Add para Multilevel Ports for Zone's IP Addresses.**

      ii. **Escriba 2049 como número de puerto y haga clic en OK.**

   d. **Haga clic en OK (Aceptar) para guardar la configuración.**

4. **Cierre Solaris Management Console.**

5. **Actualice el núcleo.**

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

▼ Cómo crear un puerto de varios niveles para una zona

Este procedimiento se utiliza cuando una aplicación que se ejecuta en una zona con etiquetas requiere un puerto de varios niveles para comunicarse con la zona. En este procedimiento, un proxy web se comunica con la zona. Para agregar el puerto de varios niveles se utiliza Solaris Management Console.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global. La zona con etiquetas debe existir. Para obtener detalles, consulte "Creating Labeled Zones" de *Trusted Extensions Configuration Guide*.

1 **Inicie Solaris Management Console.**

Para obtener detalles, consulte "Cómo administrar el sistema local con Solaris Management Console" en la página 55.

2 **Seleccione la caja de herramientas Files.**

El título de la caja de herramientas incluye `Scope=Files, Policy=TSOL`.

3 **Agregue el host proxy y el host de servicios web a la lista de equipos.**

a. **En System Configuration, diríjase hasta la herramienta Computers and Networks.**

b. **En la herramienta Computers, haga clic en el menú Action y seleccione Add Computer.**

c. **Agregue el nombre del host y la dirección IP para el host proxy.**

d. **Guarde los cambios.**

e. **Agregue el nombre del host y la dirección IP para el host de servicios web.**

f. **Guarde los cambios.**

4 **Configure la zona y el puerto de varios niveles.**

a. **Vaya a la herramienta Trusted Network Zones.**

b. **Seleccione la zona con etiquetas.**

c. **En la sección de configuración de puertos de varios niveles para las direcciones IP locales, especifique el campo de puerto y protocolo adecuado.**

d. **Guarde los cambios.**

5 **Personalice una plantilla para la zona. Para ello, realice los siguientes pasos:**

a. **Vaya a la herramienta Security Templates.**

Haga clic en el menú Action y seleccione Add Template.

b. **Utilice el nombre del host para el nombre de la plantilla.**

c. **Especifique la CIPSO para el tipo de host.**

d. **Utilice de la etiqueta de la zona para la etiqueta mínima y la etiqueta máxima.**

e. **Asigne la etiqueta de la zona al conjunto de etiquetas de seguridad.**

f. **Seleccione la ficha Hosts Explicitly Assigned.**

g. **En la sección Add an Entry, agregue la dirección IP que se asocia con la zona.**

h. **Guarde los cambios.**

6 **Cierre Solaris Management Console.**

7 **Inicie las zonas.**

```
# zoneadm -z zone-name boot
```

8 **En la zona global, agregue rutas para las nuevas direcciones.**

Por ejemplo, si las zonas comparten la dirección IP, realice lo siguiente:

```
# route add proxy labeled-zones-IP-address
# route add webservice labeled-zones-IP-address
```

◆ ◆ ◆ CAPÍTULO 11

Gestión y montaje de archivos en Trusted Extensions (tareas)

En este capítulo se describe el funcionamiento de los montajes de LOFS y de NFS en los sistemas configurados con Trusted Extensions. Además, se explica cómo realizar copias de seguridad de los archivos y cómo restaurarlos.

Uso compartido y montaje de archivos en Trusted Extensions

El software de Trusted Extensions admite los mismos sistemas de archivos y comandos de gestión de sistemas de archivos que el SO Oracle Solaris. Trusted Extensions agrega la opción de que una zona no global comparta archivos. Además, Trusted Extensions anexa una etiqueta única a cada zona no global. Todos los archivos y directorios que pertenecen a esa zona se montan en la etiqueta de la zona. Cualquier sistema de archivos compartidos que pertenezca a otras zonas o a servidores NFS se monta en la etiqueta del propietario. Trusted Extensions impide cualquier montaje que pueda infringir las políticas del control de acceso obligatorio (MAC) sobre el uso de etiquetas. Por ejemplo, la etiqueta de una zona debe dominar todas las etiquetas de su sistema de archivos montado. Solamente los sistemas de archivos con etiquetas igualmente se pueden montar con permisos de lectura y escritura.

Montajes de NFS en Trusted Extensions

Los montajes de NFS en Trusted Extensions son similares a los montajes en Oracle Solaris. Las diferencias se producen en el uso de los nombres de ruta raíz de la zona para montar una zona con etiquetas en Trusted Extensions y en la aplicación de la política de MAC.

Los recursos compartidos de NFS en Trusted Extensions son similares a los recursos compartidos de Oracle Solaris en una zona global. Sin embargo, el uso compartido de archivos desde una zona con etiquetas en un sistema de varios niveles es exclusivo de Trusted Extensions:

- **Uso compartido y montaje en la zona global:** el uso compartido y el montaje de archivos en la zona global del sistema Trusted Extensions es casi idéntico al procedimiento del SO Oracle Solaris. Para montar archivos, se pueden utilizar el montador automático, el archivo `vfstab` y el comando `mount`. Para el uso compartido de archivos, se usa el archivo `dfstab`.
- **Montaje en zonas con etiquetas**: el montaje de archivos en las zonas con etiquetas en Trusted Extensions es casi idéntico al montaje de archivos en las zonas no globales en el SO Oracle Solaris. Para montar archivos, se pueden utilizar el montador automático, el archivo `vfstab` y el comando `mount`. En Trusted Extensions, existe un único archivo de configuración `automount_home_`*etiqueta* para cada zona con etiquetas.
- **Uso compartido en zonas con etiquetas**: los archivos de una zona con etiquetas se pueden compartir en la etiqueta de la zona mediante un archivo `dfstab` que se encuentre en la etiqueta de la zona, pero que sea visible solamente para la zona global. Por lo tanto, la configuración de una zona con etiquetas para compartir archivos la realiza el administrador de la zona global en la zona global misma. Este archivo de configuración no se puede ver desde su zona con etiquetas. Para obtener más información, consulte "Procesos de la zona global y de las zonas con etiquetas" en la página 128.

Las etiquetas determinan qué archivos se pueden montar. Los archivos se comparten y se montan en una etiqueta determinada. Para que un cliente de Trusted Extensions escriba un archivo montado en NFS, el archivo debe estar montado con permisos de lectura y escritura, *y* debe estar en la misma etiqueta que el cliente. Si monta un archivo entre dos hosts de Trusted Extensions, el servidor y el cliente deben tener plantillas de hosts remotos compatibles de tipo `cipso`. Si monta un archivo entre un host de Trusted Extensions y un host sin etiquetas, los archivos que se encuentran en una sola etiqueta especificada para el host sin etiquetas en el archivo `tnrhdb` pueden montarse. Los archivos que se montan con LOFS se pueden ver, pero no se pueden modificar. Para obtener detalles sobre los montajes de NFS, consulte "Acceso a los directorios montados de NFS en Trusted Extensions" en la página 148.

Las etiquetas también determinan qué directorios y archivos pueden verse. De manera predeterminada, los objetos de nivel inferior están disponibles en un entorno de usuario. Por lo tanto, en la configuración predeterminada, los usuarios comunes pueden ver los archivos que están en la zona de un nivel inferior a su nivel actual. Por ejemplo, los usuarios pueden ver sus directorios principales de nivel inferior desde una etiqueta superior. Para obtener detalles, consulte "Creación de directorios principales en Trusted Extensions" en la página 149.

Si la seguridad del sitio prohíbe la visualización de los objetos de nivel inferior, puede hacer que los directorios de nivel inferior no sean visibles para los usuarios. Para obtener detalles, consulte "Cómo desactivar el montaje de archivos de nivel inferior" en la página 135.

La política de montaje en Trusted Extensions no incluye invalidaciones de MAC. Un proceso de etiqueta superior nunca puede modificar los archivos montados que pueden verse en una etiqueta inferior. Esta política de MAC también se aplica en la zona global. Un proceso de zona global `ADMIN_HIGH` no puede modificar un archivo montado en NFS en una etiqueta inferior, como un archivo `PUBLIC` o un archivo `ADMIN_LOW`. Las políticas de MAC aplican la configuración predeterminada y no están visibles para los usuarios comunes. Los usuarios comunes no pueden ver objetos, salvo que tengan acceso MAC.

Uso compartido de archivos desde una zona con etiquetas

En el SO Oracle Solaris, una zona no global no puede compartir los directorios de su zona. Sin embargo, en Trusted Extensions, una zona con etiquetas sí puede compartir directorios. La especificación de los directorios que se pueden compartir en una zona con etiquetas se realiza en la zona global, con un directorio que se encuentra fuera de la ruta `root` de la zona. Para obtener más información, consulte "Procesos de la zona global y de las zonas con etiquetas" en la página 128.

`/zone/`*labeled-zone*`/`*directories*	A esta ruta también se la llama ruta de la zona. Va de la zona global a la zona con etiquetas. Cada directorio en *labeled-zone* tiene la misma etiqueta que la zona.
`/zone/`*labeled-zone*`/root/`*directories*	A esta ruta también se la llama ruta raíz de la zona. Desde la perspectiva de la zona global, es la ruta `root` de una zona con etiquetas. Desde la perspectiva de la zona con etiquetas, es el root de la zona; es el directorio `/`. La zona global no usa esta ruta para administrar la zona.

Para compartir directorios desde una zona con etiquetas, el administrador de la zona global debe crear y modificar el archivo `dfstab` en el directorio `/etc` de la ruta de la zona:

```
/zone/labeled-zone/etc/dfs/dfstab
```

El directorio `/etc` no se puede ver desde la zona con etiquetas. Este directorio es diferente del directorio `/etc` que se ve desde la zona:

```
Global zone view: /zone/labeled-zone/root/etc
Labeled zone view of the same directory: /etc
```

Un archivo `dfstab` de esta ruta no activa el uso compartido de los directorios con etiquetas.

Cuando el estado de la zona con etiquetas es `ready` o `running`, los archivos que aparecen en el archivo `/zone/`*labeled-zone*`/etc/dfs/dfstab` se comparten en la etiqueta de la zona. Para conocer el procedimiento, consulte "Cómo compartir directorios desde una zona con etiquetas" en la página 153.

Acceso a los directorios montados de NFS en Trusted Extensions

De manera predeterminada, los sistemas de archivos montados en NFS son visibles en la etiqueta de sistema de archivos exportado. Si el sistema de archivos se exporta con permisos de lectura y escritura, los usuarios que cuenten con dicha etiqueta pueden escribir en los archivos. El usuario puede ver los montajes de NFS que están en una etiqueta inferior a su sesión actual, pero no puede escribir en ellos. Incluso si un sistema de archivos se comparte con permisos de lectura y escritura, el sistema de montaje puede escribirlos solamente en la etiqueta del montaje.

Para hacer que los usuarios de una zona de nivel superior puedan ver los directorios de nivel inferior montados en NFS, el administrador de la zona global del servidor NFS debe exportar el directorio principal. El directorio principal se exporta en su etiqueta. En el lado del cliente, cada zona debe tener el privilegio `net_mac_aware`. De manera predeterminada, las zonas con etiquetas incluyen el privilegio `net_mac_aware` en su conjunto `limitpriv`.

- **Configuración del servidor**: en el servidor NFS, debe exportar el directorio principal en un archivo `dfstab`. Si el directorio principal está en una zona con etiquetas, el archivo `dfstab` debe modificarse en la zona con etiquetas del directorio principal. El archivo `dfstab` para una zona con etiquetas se puede ver solamente desde la zona global. Para conocer el procedimiento, consulte "Cómo compartir directorios desde una zona con etiquetas" en la página 153.
- **Configuración del cliente**: el privilegio `net_mac_aware` debe especificarse en el archivo de configuración de la zona que se utiliza durante la etapa inicial de configuración de la zona. Por lo tanto, el usuario que tenga permiso para ver todos los directorios principales de nivel inferior también debe tener el privilegio `net_mac_aware` en cada zona, excepto en la zona más inferior. Para ver un ejemplo, consulte "Cómo montar archivos en NFS en una zona con etiquetas" en la página 155.

EJEMPLO 11–1 Cómo proporcionar acceso a los directorios principales de nivel inferior

En el servidor del directorio principal, el administrador crea y modifica el archivo `/zone/`*labeled-zone*`/etc/dfs/dfstab` en cada zona con etiquetas. El archivo `dfstab` exporta el directorio `/export/home` con permisos de lectura y escritura. De este modo, cuando el directorio se monta en la misma etiqueta, se puede escribir en el directorio principal. Para exportar el directorio `/export/home` de `PUBLIC`, el administrador crea un espacio de trabajo en la etiqueta `PUBLIC` en el servidor del directorio principal y, desde la zona global, modifica el archivo `/zone/public/etc/dfs/dfstab`.

EJEMPLO 11–1 Cómo proporcionar acceso a los directorios principales de nivel inferior *(Continuación)*

En el cliente, el administrador de la zona global comprueba que cada zona con etiquetas, excepto la etiqueta menor, tenga el privilegio `net_mac_aware`. Este privilegio permite realizar el montaje. Este privilegio se puede especificar mediante el comando `zonecfg` durante la configuración de la zona. El directorio principal de nivel inferior sólo puede verse. Mediante MAC, se impide la modificación de los archivos del directorio.

Creación de directorios principales en Trusted Extensions

Los directorios principales son un caso especial en Trusted Extensions. Debe asegurarse de que se creen los directorios principales en cada zona que los usuarios pueden utilizar. Además, deben crearse los puntos de montaje del directorio principal en las zonas del sistema del usuario. Para que los directorios principales montados en NFS funcionen correctamente, se debe usar la ubicación convencional de los directorios, `/export/home`. En Trusted Extensions, se cambió el montador automático para manejar los directorios principales en cada zona, es decir, en cada etiqueta. Para obtener detalles, consulte "Cambios en el montador automático en Trusted Extensions" en la página 150.

Los directorios principales se generan cuando se crean los usuarios. En Trusted Extensions, Solaris Management Console se utiliza para crear usuarios, por lo que la consola crea los directorios principales. Sin embargo, la consola crea los directorios principales en la zona global del servidor del directorio principal. En ese servidor, los directorios están montados con LOFS. Los directorios principales se crean automáticamente con el montador automático si se encuentran especificados como montajes LOFS.

Nota – Cuando se suprime un usuario con la consola, se suprime solamente el directorio principal del usuario en la zona global. Los directorios principales del usuario en las zonas con etiquetas no se suprimen. Usted debe encargarse de archivar y suprimir los directorios principales en las zonas con etiquetas. Para conocer el procedimiento, consulte "Cómo suprimir una cuenta de usuario de un sistema Trusted Extensions" en la página 101.

Sin embargo, el montador automático no puede crear directorios principales en servidores NFS remotos de manera automática. Primero el usuario debe iniciar sesión en el servidor NFS, o se requiere intervención administrativa. Para crear los directorios principales de los usuarios, consulte "Enable Users to Access Their Home Directories in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

Cambios en el montador automático en Trusted Extensions

En Trusted Extensions, cada una de las etiquetas requiere un montaje de directorio principal separado. Se modificó el comando `automount` a fin de gestionar los montajes automáticos con etiquetas. Para cada zona, el montador automático `autofs` monta un archivo `auto_home_`*nombre-de-zona*. Por ejemplo, a continuación se muestra la entrada para la zona global en el archivo `auto_home_global`:

```
+auto_home_global
*       -fstype=lofs    :/export/home/&
```

Cuando se inicia una zona que permite montar zonas de nivel inferior, sucede lo siguiente. Los directorios principales de las zonas de nivel inferior se montan en modo sólo lectura en `/zone/`<*nombre-de-zona*>`/export/home` . El mapa `auto_home_`<*nombre-de-zona*> especifica la ruta de `/zone` como directorio de origen para volver a realizar un montaje de `lofs` en `/zone/`< *nombre-de-zona*>`/home/`<*nombre-de-usuario*>.

Por ejemplo, a continuación se muestra una entrada `auto_home_public` en un mapa `auto_home_`*zona-en-etiqueta-superior* que se genera a partir de una zona de nivel superior:

```
+auto_home_public
*       -fstype=lofs    :/zone/public/export/home/&
```

A continuación se muestra la entrada correspondiente en la zona public:

```
auto_home_public
*       -fstype=lofs    :/export/home/&
```

Cuando se hace referencia a un directorio principal, y el nombre no coincide con ninguna de las entradas del mapa `auto_home_`<*nombre-de-zona*>, el mapa intenta encontrar la coincidencia con esta especificación de montaje en bucle de retorno. El software crea el directorio principal cuando se cumplen las dos condiciones siguientes:

1. El mapa encuentra la coincidencia con la especificación de montaje en bucle de retorno.
2. El nombre del directorio principal coincide con un usuario válido cuyo directorio principal todavía no existe en *nombre_zona*.

Para obtener detalles sobre los cambios en el montador automático, consulte la página del comando man `automount`(1M).

Software Trusted Extensions y versiones del protocolo NFS

En las versiones Solaris 10 11/06 y Solaris 10 8/07, Trusted Extensions reconoce varias etiquetas únicamente en NFS versión 4 (NFSv4). A partir de la versión Solaris 10 5/08, el software de Trusted Extensions reconoce las etiquetas de NFS versión 3 (NFSv3) y NFSv4. Puede utilizar una de las siguientes opciones de conjuntos de montaje:

```
vers=4 proto=tcp
vers=3 proto=tcp
vers=3 proto=udp
```

Trusted Extensions no tiene restricciones para los montajes realizados en protocolo `tcp`. En NFSv3 y NFSv4, el protocolo `tcp` puede usarse para los montajes de una misma etiqueta y los montajes de lectura en sentido descendente. Los montajes de lectura en sentido descendente requieren un puerto de varios niveles (MLP).

Para NFSv3, Trusted Extensions funciona como el SO Oracle Solaris. El protocolo `udp` es el que está predeterminado para NFSv3, pero `udp` se usa solamente para la operación de montaje inicial. Para las operaciones de NFS subsiguientes, el sistema utiliza `tcp`. Por lo tanto, los montajes de lectura en sentido descendente funcionan para NFSv3 con la configuración predeterminada.

Si eventualmente llegara a restringir los montajes en NFSv3 para que se use el protocolo udp en las operaciones NFS iniciales y posteriores, debe crear un MLP para las operaciones NFS que usan el protocolo `udp`. Para conocer el procedimiento, consulte "Cómo configurar un puerto de varios niveles para NFSv3 mediante `udp`" en la página 141.

Un host que está configurado con Trusted Extensions también puede compartir sus propios sistemas de archivos con hosts sin etiquetas. Un archivo o directorio que se exporta a un host sin etiquetas *se puede escribir* si su etiqueta es igual a la etiqueta asociada con el host remoto en sus entradas de base de datos de conexión de redes de confianza. Un archivo o directorio que se exporta a un host sin etiquetas *se puede leer* únicamente si su etiqueta está dominada por la etiqueta que está asociada con el host remoto.

Las comunicaciones con los sistemas que ejecutan una versión del software de Trusted Solaris son posibles en una sola etiqueta. Los sistemas Trusted Extensions y Trusted Solaris deben asignar al otro sistema una plantilla con el tipo de host sin etiquetas. Los tipos de host sin etiquetas deben especificar la misma etiqueta sola. Como cliente NFS sin etiquetas de un servidor de Trusted Solaris, la etiqueta del cliente no puede ser `ADMIN_LOW`.

El protocolo NFS que se utiliza es independiente del tipo de sistema de archivos local. En realidad, el protocolo depende del tipo de sistema operativo del equipo de uso compartido. El tipo de sistema de archivos especificado en el comando `mount` o el archivo `vfstab` para sistemas de archivos remotos siempre es NFS.

Copia de seguridad, uso compartido y montaje de archivos con etiquetas (mapa de tareas)

En el siguiente mapa de tareas, se describen las tareas comunes que se emplean para realizar copias de seguridad y restaurar los datos de sistemas de archivos con etiquetas y para compartir o montar los directorios y archivos que tienen etiquetas.

Tarea	Descripción	Para obtener instrucciones
Realizar copias de seguridad de archivos.	Proteger los datos con una copia de seguridad.	"Cómo realizar copias de seguridad de los archivos en Trusted Extensions" en la página 152
Restaurar datos.	Restaurar datos de una copia de seguridad.	"Cómo restaurar archivos en Trusted Extensions" en la página 153
Compartir el contenido de un directorio desde una zona con etiquetas.	Compartir el contenido de un directorio con etiquetas con los usuarios.	"Cómo compartir directorios desde una zona con etiquetas" en la página 153
Montar el contenido de un directorio compartido por una zona con etiquetas.	Montar el contenido de un directorio en una zona en la misma etiqueta en modo de lectura y escritura. Cuando una zona de nivel superior monta el directorio compartido, el directorio se monta en modo de sólo lectura.	"Cómo montar archivos en NFS en una zona con etiquetas" en la página 155
Crear puntos de montaje del directorio principal.	Se crean puntos de montaje para cada usuario en cada etiqueta. Esta tarea permite a los usuarios acceder a su directorio principal en un sistema que no sea el servidor del directorio principal de NFS.	"Enable Users to Access Their Home Directories in Trusted Extensions" de *Trusted Extensions Configuration Guide*
Ocultar información de nivel inferior a un usuario que trabaja en una etiqueta superior.	Impedir la visualización de información de nivel inferior desde una ventana de nivel superior.	"Cómo desactivar el montaje de archivos de nivel inferior" en la página 135
Resolver problemas de montaje de sistema de archivos.	Resolver problemas relacionados con el montaje de un sistema de archivos.	"Cómo resolver problemas por fallos de montaje en Trusted Extensions" en la página 160

▼ Cómo realizar copias de seguridad de los archivos en Trusted Extensions

1 Asuma el rol de operador.

Este rol incluye el perfil de derechos de las copias de seguridad de medios.

2 Utilice uno de los siguientes métodos para realizar copias de seguridad:

- `/usr/lib/fs/ufs/ufsdump` para las copias principales
- `/usr/sbin/tar cT` para las copias pequeñas
- Una secuencia de comandos que llame a cualquiera de estos comandos

  Por ejemplo, la aplicación para realizar copias de seguridad Budtool llama al comando `ufsdump`. Consulte la página del comando man `ufsdump`(1M). Para obtener detalles sobre la opción `T` para el comando `tar`, consulte la página del comando man `tar`(1).

▼ Cómo restaurar archivos en Trusted Extensions

1 Conviértase en usuario root.

2 Utilice uno de los métodos siguientes:

- `/usr/lib/fs/ufs/ufsrestore` para restauraciones principales
- `/usr/sbin/tar xT` para restauraciones pequeñas
- Una secuencia de comandos que llame a cualquiera de estos comandos

Para obtener detalles sobre la opción `T` para el comando `tar`, consulte la página del comando man `tar`(1).



Precaución – Sólo estos comandos preservan las etiquetas.

▼ Cómo compartir directorios desde una zona con etiquetas

Como en el SO Oracle Solaris, la herramienta Mounts and Shares de Solaris Management Console se utiliza para compartir y montar archivos desde la zona global. Esta herramienta no se puede usar para montar o compartir directorios que se originen en zonas con etiquetas. Cree un archivo `dfstab` en la etiqueta de la zona y, a continuación, reinicie la zona para compartir los directorios con etiquetas.



Precaución – No utilice nombres propietarios para los sistemas de archivos compartidos. Los nombres de los sistemas de archivos compartidos son visibles para todos los usuarios.

Antes de empezar Debe ser superusuario o asumir el rol de administrador del sistema en la zona global del servidor de archivos.

1 **Cree un espacio de trabajo en la etiqueta del directorio que se va a compartir.**

Para obtener detalles, consulte "How to Add a Workspace at a Particular Label" de *Trusted Extensions User's Guide*.

2 **Cree un archivo `dfstab` en la etiqueta de la zona.**

Para cada zona que comparta un directorio, repita los pasos siguientes:

a. **Cree el directorio `/etc/dfs` en la zona.**

```
# mkdir -p /zone/zone-name/etc/dfs
```

b. **Abra el editor de confianza.**

Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

c. **Escriba el nombre de ruta completo del archivo `dfstab` en el editor.**

```
# /zone/zone-name/etc/dfs/dfstab
```

d. **Agregue una entrada para compartir un directorio desde esa zona.**

La entrada describe el directorio desde la perspectiva de la ruta raíz de la zona. Por ejemplo, la siguiente entrada comparte los archivos de una aplicación en la etiqueta de la zona contenedora:

```
share -F nfs -o ro /viewdir/viewfiles
```

3 **Inicie cada zona para compartir los directorios.**

En la zona global, ejecute uno de los siguientes comandos para cada zona. Cada zona puede compartir sus directorios de cualquiera de estas maneras. El uso compartido real tiene lugar cuando las zonas están en estado `ready` o `running`.

- **Si la zona no está en estado running, y no desea que los usuarios inicien sesión en el servidor en la etiqueta de la zona, fije el estado de la zona en `ready`.**

```
# zoneadm -z zone-name ready
```

- **Si la zona no está en estado running, y los usuarios tienen permiso para iniciar sesión en el servidor en la etiqueta de la zona, dé inicio a la zona.**

```
# zoneadm -z zone-name boot
```

- **Si la zona ya está en ejecución, reiníciela.**

```
# zoneadm -z zone-name reboot
```

4 **Muestre los directorios que se comparten desde el sistema.**

```
# showmount -e
```

5 **Para activar el cliente para montar los archivos exportados, consulte** **"Cómo montar archivos en NFS en una zona con etiquetas" en la página 155****.**

Ejemplo 11–2 Uso compartido del directorio `/export/share` en la etiqueta `PUBLIC`

Para las aplicaciones que se ejecutan en la etiqueta `PUBLIC`, el administrador del sistema permite a los usuarios leer la documentación del directorio `/export/share` de la zona `public`. La zona denominada `public` se ejecuta en la etiqueta `PUBLIC`.

Primero, el administrador crea un espacio de trabajo `public` y edita el archivo `dfstab`.

```
# mkdir -p /zone/public/etc/dfs
# /usr/dt/bin/trusted_edit /zone/public/etc/dfs/dfstab
```

En el archivo, el administrador agrega la siguiente entrada:

```
## Sharing PUBLIC user manuals
share -F nfs -o ro /export/appdocs
```

El administrador deja el espacio de trabajo `public` y vuelve al espacio de trabajo de Trusted Path. Dado que los usuarios no tienen permiso para iniciar sesión en este sistema, el administrador comparte los archivos. Para ello, pone la zona en el estado ready:

```
# zoneadm -z public ready
```

Los usuarios pueden acceder a los directorios compartidos una vez que éstos quedan montados en sus sistemas.

▼ Cómo montar archivos en NFS en una zona con etiquetas

En Trusted Extensions, las zonas con etiquetas gestionan el montaje de los archivos en su zona.

Los archivos de hosts con etiquetas y sin etiquetas pueden montarse en un host con etiquetas de Trusted Extensions.

- Para montar los archivos de lectura y escritura desde un host de una sola etiqueta, la etiqueta asignada del host remoto debe ser idéntica a la zona en que se monta el archivo.
- Los archivos que se montan en una zona de nivel superior son de sólo lectura.
- En Trusted Extensions, el archivo de configuración `auto_home` se personaliza por zona. El archivo se denomina según el nombre de la zona. Por ejemplo, si el sistema tiene una zona global y una zona public, habrá dos archivos `auto_home`: `auto_home_global` y `auto_home_public`.

Trusted Extensions utiliza las mismas interfaces de montaje que el SO Oracle Solaris:

- Para montar archivos durante el inicio, utilice el archivo `/etc/vfstab` en la zona con etiquetas.
- Para montar los archivos dinámicamente, utilice el comando `mount` en la zona con etiquetas.
- Para montar los directorios principales automáticamente, utilice los archivos `auto_home_`*nombre-de-zona*.
- Para montar otros directorios automáticamente, use los mapas de montaje automático estándares. Si los mapas de montaje automático están en LDAP, utilice los comandos LDAP para gestionarlos.

Antes de empezar Debe estar en el sistema cliente, en la zona de la etiqueta de los archivos que desea montar. Si no usa el montador automático, debe ser superusuario o estar en el rol de administrador del sistema. Para montar servidores de nivel inferior, la zona debe estar configurada con el privilegio `net_mac_aware`.

● **Para montar archivos en NFS en una zona con etiquetas, aplique los procedimientos siguientes.**

La mayoría de los procedimientos requieren la creación de un espacio de trabajo en una etiqueta determinada. Para crear un espacio de trabajo, consulte "How to Add a Workspace at a Particular Label" de *Trusted Extensions User's Guide*.

- **Monte los archivos dinámicamente.**

  En la zona con etiquetas, utilice el comando `mount`. Para ver un ejemplo sobre cómo montar archivos dinámicamente, consulte el Ejemplo 11–3.

- **Monte los archivos cuando se inicie la zona**

  En la zona con etiquetas, agregue los montajes al archivo `vfstab`.

  Para ver ejemplos sobre cómo montar archivos cuando se inicia la zona con etiquetas, consulte el Ejemplo 11–4 y el Ejemplo 11–5.

- **Monte los directorios principales en los sistemas que se administran con LDAP.**

  a. **En cada etiqueta, agregue las especificaciones de usuario en los archivos `auto_home_`*nombre-de-zona*.**

  b. **A continuación, utilice estos archivos para rellenar la base de datos `auto_home_`*nombre-de-zona* en el servidor LDAP.**

  Si desea ver un ejemplo, consulte el Ejemplo 11–6.

- **Monte los directorios principales en sistemas que se administran con los archivos.**

  a. **Cree y rellene un archivo `/export/home/auto_home_`*nombre-de-zona-con-etiqueta-inferior*.**

  b. **Edite el archivo `/etc/auto_home_`*nombre-de-zona-con-etiqueta-inferior* a fin de que señale al archivo que recién se rellenó.**

  c. **Modifique el archivo `/etc/auto_home_`*nombre-de-zona-con-etiqueta-inferior* en cada zona de nivel superior a fin de que apunte al archivo que creó en el Paso a.**

  Si desea ver un ejemplo, consulte el Ejemplo 11–7.

Ejemplo 11–3 Montaje de archivos en una zona con etiquetas con el comando `mount`

En este ejemplo, el administrador del sistema monta un sistema de archivos remoto desde una zona public. La zona public está en un servidor de varios niveles.

Después de asumir el rol de administrador del sistema, el administrador crea un espacio de trabajo en la etiqueta `PUBLIC`. En ese espacio de trabajo, el administrador ejecuta el comando `mount`.

```
# zonename
public
# mount -F nfs remote-sys:/zone/public/root/opt/docs  /opt/docs
```

El servidor de archivos de una sola etiqueta en la etiqueta `PUBLIC` también contiene documentos que se deben montar:

```
# mount -F nfs public-sys:/publicdocs  /opt/publicdocs
```

Cuando la zona public del servidor de archivos `remote-sys` se encuentra en estado `ready` o `running`, los archivos `remote-sys` se montan correctamente en este sistema. Cuando el servidor de archivos `public-sys` se está ejecutando, los archivos se montan correctamente.

Ejemplo 11–4 Montaje de archivos de lectura y escritura en una zona con etiquetas mediante la modificación del archivo `vfstab`

En este ejemplo, el administrador del sistema monta dos sistemas de archivos remotos en la etiqueta `PUBLIC` en la zona public del sistema local cuando esta zona se inicia. Uno de los montajes de sistema de archivos es de un sistema de varios niveles y el otro, de un sistema de una sola etiqueta.

Después de asumir el rol de administrador del sistema, el administrador crea un espacio de trabajo en la etiqueta `PUBLIC`. En ese espacio de trabajo, el administrador modifica el archivo `vfstab` en la zona.

```
## Writable books directories at PUBLIC
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  rw
public-sys:/publicdocs    - /opt/publicdocs  nfs no yes rw
```

Para acceder a los archivos en la zona con etiquetas remota del sistema de varios niveles, la entrada `vfstab` utiliza la ruta raíz de la zona de la zona public del sistema remoto, `/zone/public/root`, como nombre de ruta de los directorios que se deben montar. La ruta del sistema de una sola etiqueta es idéntica a la ruta que se utilizaría en un sistema Oracle Solaris.

El administrador monta los archivos en una ventana de terminal en la etiqueta `PUBLIC`.

```
# mountall
```

Ejemplo 11–5 Montaje de archivos de nivel inferior en una zona con etiquetas mediante la modificación del archivo `vfstab`

En este ejemplo, el administrador del sistema monta un sistema de archivos remoto de una zona public en la zona interna del sistema local. Después de asumir el rol de administrador del sistema, el administrador crea un espacio de trabajo en la etiqueta `INTERNAL`. Luego, modifica el archivo `vfstab` en esa zona.

```
## Readable books directory at PUBLIC
## ro entry indicates that PUBLIC docs can never be mounted rw in internal zone
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  ro
```

Para acceder a los archivos en la zona con etiquetas remota, la entrada `vfstab` utiliza la ruta raíz de la zona de la zona public del sistema remoto, `/zone/public/root`, como nombre de ruta de los directorios que se deben montar.

Desde la perspectiva de un usuario en la zona interna, se puede acceder a los archivos en `/opt/docs`.

En una ventana de terminal, en la etiqueta `INTERNAL`, el administrador monta los archivos.

```
# mountall
```

Ejemplo 11–6 Montaje de directorios principales con etiquetas de una red que se administra mediante LDAP

En este ejemplo, el administrador del sistema activa a un usuario nuevo, `ikuk`, para que acceda a su directorio principal en cada etiqueta. Este sitio utiliza dos servidores de directorios principales y se administra mediante LDAP. El segundo servidor contiene los directorios principales para los usuarios `jdoe` y `pkai`. El usuario nuevo se agrega a esta lista.

Primero, después de asumir el rol de administrador del sistema, el administrador modifica los archivos `auto_home_`*nombre-de-zona* en el directorio `/etc` de la zona global a fin de incluir al usuario nuevo en el segundo servidor del directorio principal.

```
## auto_home_global file
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&

## auto_home_internal file
## Mount the home directory from the internal zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&

## auto_home_public
## Mount the home directory from the public zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

Luego, a fin de activar a los usuarios para que inicien sesión en todas las etiquetas, el administrador repite estas ediciones en los archivos `auto_home_`*nombre-de-zona* de cada etiqueta.

Por último, después de modificar cada archivo `auto_home_`*nombre-de-zona* de este sistema, el administrador utiliza estos archivos para agregar entradas a la base de datos LDAP.

De manera similar a como sucede en el SO Oracle Solaris, la entrada `+auto_home_public` de los archivos `/etc/auto_home_`*nombre-de-zona* dirige el montador automático a las entradas LDAP. Los archivos `auto_home_`*nombre-de-zona* en otros sistemas de la red se actualizan desde la base de datos LDAP.

Ejemplo 11–7 Montaje de un directorio principal de nivel inferior en un sistema que se administra mediante archivos

En este ejemplo, el administrador del sistema activa a los usuarios para que accedan a sus directorios principales en cada etiqueta. Las etiquetas del sitio son `PUBLIC`, `INTERNAL` y `NEEDTOKNOW`. Este sitio utiliza dos servidores de directorios principales y se administra mediante el uso de archivos. El segundo servidor contiene los directorios principales para los usuarios `jdoe` y `pkai`.

Para completar esta tarea, el administrador del sistema define los directorios principales NFS de la zona public y comparte esta configuración con las zonas internal y needtoknow.

En primer lugar, después de asumir el rol de administrador del sistema, el administrador crea un espacio de trabajo en la etiqueta `PUBLIC`. En este espacio de trabajo, el administrador crea un archivo nuevo, `/export/home/auto_home_public`. Este archivo contiene todas las entradas de especificación NFS personalizadas por usuario.

```
## /export/home/auto_home_public file at PUBLIC label
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
*      homedir-server:/export/home/&
```

En segundo lugar, el administrador modifica el archivo `/etc/auto_home_public` a fin de que apunte a este archivo nuevo.

```
## /etc/auto_home_public file in the public zone
## Use /export/home/auto_home_public for the user entries
## +auto_home_public
+ /export/home/auto_home_public
```

Esta entrada le indica al montador automático que utilice el contenido del archivo local.

En tercer lugar, el administrador modifica, de manera similar, el archivo `/etc/auto_home_public` archivo en las zonas internal y needtoknow. El administrador utiliza el nombre de la ruta de la zona public que está visible para las zonas internal y needtoknow.

```
## /etc/auto_home_public file in the internal zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public
```

```
## /etc/auto_home_public file in the needtoknow zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public
```

Cuando el administrador agrega al usuario nuevo `ikuk`, éste se agrega en el archivo `/export/home/auto_home_public` de la etiqueta `PUBLIC`.

```
## /export/home/auto_home_public file at PUBLIC label
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

Las zonas de nivel superior leen en sentido descendente para obtener directorios principales por usuario de la zona public de nivel inferior.

▼ Cómo resolver problemas por fallos de montaje en Trusted Extensions

Antes de empezar Debe estar en la zona de la etiqueta de los archivos que desea montar. Debe ser superusuario o estar en el rol de administrador del sistema.

1 **Compruebe los atributos de seguridad del servidor NFS.**

Utilice la herramienta Security Templates de Solaris Management Console en el ámbito adecuado. Para obtener detalles, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

a. **Compruebe que la dirección IP del servidor NFS sea un host asignado en una de las plantillas de seguridad.**

La dirección se puede asignar de manera directa o de manera indirecta, mediante un mecanismo comodín. La dirección puede estar en una plantilla con etiquetas o sin etiquetas.

b. **Revise la etiqueta que la plantilla asigna al servidor NFS.**

Esta etiqueta debe ser coherente con la etiqueta en la que intenta montar los archivos.

2 **Revise la etiqueta de la zona actual.**

Si esta etiqueta es superior a la etiqueta del sistema de archivos montados, no podrá escribir en el montaje, aunque el sistema de archivos remoto se exporte con permisos de lectura y escritura. Sólo puede escribir en el sistema de archivos montados, en la etiqueta del montaje.

3 **Para montar los sistemas de archivos desde un servidor NFS que ejecuta versiones anteriores del software Trusted Solaris, realice las siguientes acciones:**

- **Para un servidor NFS de Trusted Solaris 1, use las opciones `vers=2` y `proto=udp` para el comando `mount`.**
- **Para un servidor NFS de Trusted Solaris 2.5.1, use las opciones `vers=2` y `proto=udp` para el comando `mount`.**
- **Para un servidor NFS de Trusted Solaris 8, use las opciones `vers=3` y `proto=udp` para el comando `mount`.**

Para montar sistemas de archivos de cualquiera de estos servidores, el servidor debe estar asignado a una plantilla sin etiquetas.

◆ ◆ ◆ CAPÍTULO 12

Redes de confianza (descripción general)

En este capítulo, se describen los conceptos y los mecanismos de las redes de confianza de Trusted Extensions.

La red de confianza

Trusted Extensions asigna atributos de seguridad a las zonas, los hosts y las redes. Estos atributos garantizan que las siguientes funciones de seguridad se apliquen en la red:

- Los datos tienen las etiquetas correctas en las comunicaciones de red.
- Las reglas de control de acceso obligatorio (MAC) se aplican cuando se envían o se reciben datos mediante una red local, y cuando se montan los sistemas de archivos.
- Las reglas de MAC se aplican cuando se enrutan datos a redes distantes.
- Las reglas de MAC se aplican cuando se enrutan datos a zonas.

En Trusted Extensions, MAC protege los paquetes de red. Las etiquetas se utilizan para las decisiones de MAC. Los datos se etiquetan explícita o implícitamente con una etiqueta de sensibilidad. La etiqueta tiene un campo de ID, un campo de clasificación o "nivel" y un campo de compartimiento o "categoría". Los datos deben someterse a una comprobación de acreditación. Esta comprobación determina si la etiqueta está bien formada y si se encuentra dentro del rango de acreditación del host de recepción. Los paquetes bien formados que están dentro del rango de acreditación del host de recepción obtienen acceso.

Es posible etiquetar los paquetes IP que se intercambian entre los sistemas de confianza. Trusted Extensions admite las etiquetas de opción de seguridad de IP comercial (CIPSO). La

etiqueta CIPSO de un paquete sirve para clasificar, separar y enrutar paquetes IP. Las decisiones de enrutamiento comparan la etiqueta de sensibilidad de los datos con la etiqueta del destino.

Por lo general, en una red de confianza, el host de envío genera la etiqueta y el host de recepción la procesa. Sin embargo, un enrutador de confianza también puede agregar o filtrar etiquetas cuando reenvía paquetes en una red de confianza. Antes de la transmisión, se asigna una etiqueta de sensibilidad a una etiqueta CIPSO. La etiqueta CIPSO está integrada en el paquete IP. En general, el remitente y el receptor de un paquete operan en la misma etiqueta.

El software de las redes de confianza garantiza que la política de seguridad de Trusted Extensions se aplique incluso cuando los sujetos (procesos) y los objetos (datos) estén en hosts diferentes. Las redes de Trusted Extensions mantienen el MAC en todas las aplicaciones distribuidas.

Paquetes de datos de Trusted Extensions

Los paquetes de datos de Trusted Extensions incluyen una opción de etiqueta CIPSO. Los paquetes de datos pueden enviarse mediante las redes IPv4 o IPv6.

En el formato IPv4 estándar, el encabezado IPv4 con opciones va seguido de un encabezado TCP, UDP o SCTP, y, a continuación, los datos reales. La versión de Trusted Extensions de un paquete IPv4 utiliza la opción CIPSO del encabezado IP para los atributos de seguridad.

Encabezado IPv4 con opción CIPSO	TCP, UDP o SCTP	Datos

En el formato IPv6 estándar, un encabezado IPv6 con extensiones va seguido de un encabezado TCP, UDP o SCTP, y, a continuación, los datos reales. El paquete IPv6 de Trusted Extensions incluye una opción de seguridad de varios niveles en el encabezado con extensiones.

Encabezado IPv6 con extensiones	TCP, UDP o SCTP	Datos

Comunicaciones de la red de confianza

Trusted Extensions admite hosts con etiquetas y sin etiquetas en una red de confianza. LDAP es un servicio de nombres completamente admitido. Varios comandos e interfaces gráficas de usuario permiten la administración de la red.

Los sistemas que ejecutan el software de Trusted Extensions admiten las comunicaciones de red entre los hosts de Trusted Extensions y cualquiera de los siguientes tipos de sistemas:

- Otros sistemas que ejecutan Trusted Extensions
- Los sistemas que ejecutan sistemas operativos que no reconocen atributos de seguridad, pero admiten TCP/IP, como los sistemas de Oracle Solaris, otros sistemas UNIX, Microsoft Windows y Macintosh OS
- Los sistemas que ejecutan otros sistemas operativos de confianza que reconocen etiquetas CIPSO

Como en el SO Oracle Solaris, el servicio de nombres puede administrar las comunicaciones y los servicios de red de Trusted Extensions. Trusted Extensions agrega las siguientes interfaces a las interfaces de red de Oracle Solaris:

- Trusted Extensions agrega tres bases de datos de configuración de la red: `tnzonecfg`, `tnrhdb` y `tnrhtp`. Para obtener detalles, consulte "Bases de datos de configuración de red en Trusted Extensions" en la página 166.
- La versión de Trusted Extensions del archivo de cambio del servicio de nombres, `nsswitch.conf`, incluye entradas para las bases de datos `tnrhtp` y `tnrhdb`. Es posible modificar estas entradas para que se adapten a la configuración de cada sitio.

  Trusted Extensions utiliza el servicio de nombres LDAP para gestionar de manera centralizada los archivos de configuración que definen los hosts, las redes y los usuarios. Las entradas `nsswitch.conf` predeterminadas para las bases de datos de la red de confianza del servicio de nombres LDAP son las siguientes:

  ```
  # Trusted Extensions
  tnrhtp: files ldap
  tnrhdb: files ldap
  ```

  El servicio de nombres LDAP en Oracle Directory Server Enterprise Edition es el único servicio de nombres completamente admitido en Trusted Extensions. Para obtener información sobre el uso de LDAP en un sistema que está configurado con Trusted Extensions, consulte el Capítulo 9, "Trusted Extensions y LDAP (descripción general)".
- Trusted Extensions agrega herramientas a Solaris Management Console. Se utiliza la consola para gestionar zonas, hosts y redes de manera centralizada. En "Herramientas de Solaris Management Console" en la página 38, se describen las herramientas de red.

  En la *Trusted Extensions Configuration Guide* , se describe cómo definir zonas y hosts cuando se configura la red. Para obtener más detalles, consulte el Capítulo 13, "Gestión de redes en Trusted Extensions (tareas)".
- Trusted Extensions agrega comandos para administrar las redes de confianza. Trusted Extensions también agrega opciones a los comandos de red de Oracle Solaris. Para obtener una descripción de estos comandos, consulte "Comandos de red en Trusted Extensions" en la página 167.

Bases de datos de configuración de red en Trusted Extensions

Trusted Extensions carga tres bases de datos de configuración de red en el núcleo. Estas bases de datos se utilizan en las comprobaciones de acreditaciones cuando se transmiten los datos de un host a otro.

- `tnzonecfg`: esta base de datos local almacena atributos de la zona que están relacionados con la seguridad. Los atributos de cada zona especifican la etiqueta de la zona y el acceso de dicha zona a los puertos de un solo nivel y de varios niveles. Otro atributo gestiona las respuestas a los mensajes de control, como `ping`. Las etiquetas de las zonas se definen en el archivo `label_encodings`. Para obtener más información, consulte las páginas del comando man `label_encodings(4)` y `smtnzonecfg(1M)`. Para ver una explicación sobre los puertos de varios niveles, consulte "Zonas y puertos de varios niveles" en la página 127.
- `tnrhtp`: esta base de datos almacena plantillas que describen los atributos de seguridad de los hosts y las puertas de enlace. `tnrhtp` puede tratarse de una base de datos local o almacenada en el servidor LDAP. Los hosts y las puertas de enlace utilizan los atributos del host de destino y la puerta de enlace del próximo salto para aplicar el MAC al enviar tráfico. Cuando el tráfico se recibe, los hosts y las puertas de enlace utilizan los atributos del remitente. Para obtener detalles sobre los atributos de seguridad, consulte "Atributos de seguridad de la red de confianza" en la página 168. Para obtener más información, consulte la página del comando man `smtnrhtp(1M)`.
- `tnrhdb`: esta base de datos contiene los prefijos de red (mecanismo de reserva) y las direcciones IP que corresponden a todos los hosts que tienen permiso para comunicarse. `tnrhdb` puede ser una base de datos local o una almacenada en el servidor LDAP. Se asigna una plantilla de seguridad de la base de datos `tnrhtp` a cada host o prefijo de red. Los atributos de la plantilla definen los atributos del host asignado. Para obtener más información, consulte la página del comando man `smtnrhdb(1M)`.

En Trusted Extensions, se amplió Solaris Management Console para gestionar estas bases de datos. Para obtener detalles, consulte "Herramientas de Solaris Management Console" en la página 38.

Comandos de red en Trusted Extensions

Trusted Extensions agrega los siguientes comandos para administrar las redes de confianza:

- `tnchkdb`: este comando se utiliza para comprobar la precisión de las bases de datos de la red de confianza. El comando `tnchkdb` se utiliza cuando se modifica una plantilla de seguridad (`tnrhtp`), una asignación de plantilla de seguridad (`tnrhdb`) o la configuración de una zona (`tnzonecfg`). Las herramientas de Solaris Management Console ejecutan este comando automáticamente cuando se modifica una base de datos. Para obtener detalles, consulte la página del comando man `tnchkdb`(1M).
- `tnctl`: este comando puede utilizarse para actualizar la información de la red de confianza en el núcleo. `tnctl` también es un servicio del sistema. Cuando se reinicia con el comando `svcadm restart /network/tnctl`, se refresca la caché del núcleo de las bases de datos de la red de confianza en el sistema local. Las herramientas de Solaris Management Console ejecutan este comando automáticamente cuando se modifica una base de datos en el ámbito Files. Para obtener detalles, consulte la página del comando man `tnctl`(1M).
- `tnd`: este daemon extrae la información de `tnrhdb` y `tnrhtp` del directorio LDAP y los archivos locales. La información de los servicios de nombres se carga por orden en el archivo `nsswitch.conf`. En el momento del inicio, el servicio `svc:/network/tnd` inicia el daemon `tnd`. Este servicio depende de `svc:/network/ldap/client`.

  El comando `tnd` también puede utilizarse para la depuración y para cambiar el intervalo de sondeo. Para obtener detalles, consulte la página del comando man `tnd`(1M).
- `tninfo`: este comando muestra los detalles del estado actual de la caché del núcleo de la red de confianza. Es posible filtrar los resultados por zona, plantilla de seguridad o nombre de host. Para obtener detalles, consulte la página del comando man `tninfo`(1M).

Trusted Extensions agrega opciones a los siguientes comandos de red de Oracle Solaris:

- `ifconfig`: el indicador de interfaz `all-zones` de este comando pone la interfaz especificada a disposición de todas las zonas del sistema. La zona adecuada para entregar los datos se encuentra determinada por la etiqueta que está asociada con los datos. Para obtener detalles, consulte la página del comando man `ifconfig`(1M).
- `netstat`: la opción `-R` amplía el uso de `netstat` de Oracle Solaris para mostrar información específica de Trusted Extensions, como los atributos de seguridad para sockets de varios niveles y las entradas de la tabla de enrutamiento. Los atributos de seguridad ampliados incluyen la etiqueta del igual y establecen si el socket es específico para una zona o si está disponible para varias zonas. Para obtener detalles, consulte la página del comando man `netstat`(1M).
- `route`: la opción `-secattr` amplía el uso de `route` de Oracle Solaris para mostrar los atributos de seguridad de la ruta. El valor de la opción tiene el siguiente formato:

  `min_sl=`*label*`,max_sl=`*label*`,doi=`*integer*`,cipso`

  La palabra clave `cipso` es opcional y se establece de manera predeterminada. Para obtener detalles, consulte la página del comando man `route`(1M).

- `snoop`: como en el SO Oracle Solaris, puede utilizarse la opción `-v` de este comando para mostrar los encabezados IP de manera más detallada. En Trusted Extensions, los encabezados contienen información de la etiqueta.

Atributos de seguridad de la red de confianza

La administración de redes en Trusted Extensions se basa en plantillas de seguridad. Una plantilla de seguridad describe un conjunto de hosts que tienen protocolos comunes y atributos de seguridad idénticos.

Los atributos de seguridad se asignan administrativamente a los sistemas, tanto los hosts como los enrutadores, mediante plantillas. El administrador de la seguridad administra las plantillas y las asigna a los sistemas. Si un sistema no tiene una plantilla asignada, no se permiten las comunicaciones con ese sistema.

Cada plantilla recibe un nombre e incluye lo siguiente:

- Un tipo de host, que puede ser sin etiquetas o CIPSO. El tipo de host de la plantilla determina el protocolo que se utiliza para las comunicaciones de red.

  El tipo de host se utiliza para determinar si se usan o no las opciones CIPSO y afecta al MAC. Consulte "Tipo de host y nombre de plantilla en plantillas de seguridad" en la página 169.
- Un conjunto de atributos de seguridad que se aplican a cada tipo de host.

Para obtener más detalles sobre los tipos de hosts y los atributos de seguridad, consulte "Atributos de seguridad de red en Trusted Extensions" en la página 168.

Atributos de seguridad de red en Trusted Extensions

Trusted Extensions se instala con un conjunto predeterminado de plantillas de seguridad. Cuando se asigna una plantilla a un host, los valores de seguridad de la plantilla se aplican al host. En Trusted Extensions, mediante una plantilla, se asignan atributos de seguridad a los hosts con etiquetas y sin etiquetas de la red. No es posible acceder a los hosts que no tienen una plantilla de seguridad asignada. Las plantillas pueden almacenarse localmente o en el servicio de nombres LDAP en Oracle Directory Server Enterprise Edition.

Las plantillas pueden asignarse directamente o indirectamente a un host. La asignación directa asigna una plantilla a una dirección IP específica. La asignación indirecta asigna una plantilla a una dirección de red que incluye el host. Los hosts que no tienen una plantilla de seguridad no pueden comunicarse con los hosts que están configurados con Trusted Extensions. Para obtener una explicación sobre la asignación directa e indirecta, consulte "Mecanismo de reserva de la red de confianza" en la página 171.

Las plantillas se crean o se modifican con la herramienta Security Templates de Solaris Management Console. La herramienta Security Templates hace que se completen los campos que sean necesarios en las plantillas. El tipo de host determina qué campos son necesarios.

Cada tipo de host tiene su propio conjunto de atributos de seguridad adicionales, tanto necesarios como opcionales. Los siguientes atributos de seguridad están especificados en las plantillas de seguridad:

- **Tipo de host**: define si los paquetes tienen etiquetas de seguridad CIPSO o no tienen ningún tipo de etiquetas.
- **Etiqueta predeterminada**: define el nivel de confianza del host sin etiquetas. En esta etiqueta, el host o la puerta de enlace de recepción de Trusted Extensions leen los paquetes que se envían mediante un host sin etiquetas.

  El atributo de la etiqueta predeterminada es específico del tipo de host sin etiquetas. Para obtener detalles, consulte la página del comando man `smtnrhtp(1M)` y las secciones siguientes.
- **DOI**: es un entero positivo, distinto de cero, que identifica el dominio de interpretación. El DOI se utiliza para indicar qué conjunto de codificaciones de etiqueta se aplica a una comunicación o entidad de red. Las etiquetas con DOI diferentes están separadas, incluso si son idénticas en todo lo demás. En los hosts unlabeled , el DOI se aplica a la etiqueta predeterminada. En Trusted Extensions, el valor predeterminado es `1`.
- **Etiqueta mínima**: define el nivel más bajo del rango de acreditación de etiquetas. Los hosts y las puertas de enlace del próximo salto no reciben paquetes que estén por debajo de la etiqueta mínima que está especificada en la plantilla correspondiente.
- **Etiqueta máxima**: define el nivel más alto del rango de acreditación de etiquetas. Los hosts y las puertas de enlace del próximo salto no reciben paquetes que estén por encima de la etiqueta máxima que está especificada en la plantilla correspondiente.
- **Conjunto de etiquetas de seguridad**: es opcional. Especifica un conjunto discreto de etiquetas de seguridad para una plantilla de seguridad. Además del rango de acreditación correspondiente que se encuentra determinado por la etiqueta máxima y la etiqueta mínima, los hosts que se asignan a una plantilla con un conjunto de etiquetas de seguridad pueden enviar y recibir paquetes que coincidan con cualquiera de las etiquetas del conjunto de etiquetas. El número máximo de etiquetas que puede especificarse es cuatro.

Tipo de host y nombre de plantilla en plantillas de seguridad

Trusted Extensions admite dos tipos de hosts en las bases de datos de la red de confianza y proporciona dos plantillas predeterminadas:

- **Tipo de host CIPSO**: diseñado para los host que ejecutan sistemas operativos de confianza. Trusted Extensions suministra la plantilla denominada `cipso` para este tipo de host.

  El protocolo de la opción de seguridad de IP común (CIPSO) se utiliza para especificar las etiquetas de seguridad que se transfieren en el campo de opciones IP. Las etiquetas CIPSO se obtienen automáticamente de la etiqueta de datos. El tipo de etiqueta 1 se utiliza para

transferir la etiqueta de seguridad CIPSO. Esta etiqueta se utiliza para realizar comprobaciones de seguridad en el nivel IP y para asignar una etiqueta a los datos del paquete de red.

- **Tipo de host sin etiquetas**: está diseñado para los hosts que utilizan protocolos de redes estándar, pero que no admiten opciones CIPSO. Trusted Extensions suministra la plantilla denominada `admin_low` para este tipo de host.

  Se asigna este tipo de host a los hosts que ejecutan el SO Oracle Solaris u otros sistemas operativos sin etiquetas. Este tipo de host proporciona una etiqueta y una acreditación predeterminadas para aplicar a las comunicaciones con el host sin etiquetas. Además, se puede especificar un rango de etiquetas o un conjunto de etiquetas discretas para permitir el envío de paquetes a una puerta de enlace sin etiquetas para el posterior reenvío.



Precaución – La plantilla `admin_low` brinda un ejemplo para la creación de plantillas sin etiquetas con etiquetas específicas del sitio. Mientras que la plantilla `admin_low` es necesaria para la instalación de Trusted Extensions, puede que las configuraciones de seguridad no sean adecuadas para las operaciones habituales del sistema. Conserve las plantillas proporcionadas sin modificaciones para el mantenimiento del sistema y el soporte técnico.

Etiqueta predeterminada en plantillas de seguridad

Las plantillas para el tipo de host sin etiquetas especifican una etiqueta predeterminada. Esta etiqueta se utiliza para controlar las comunicaciones con los hosts cuyos sistemas operativos no reconocen etiquetas, como los sistemas Oracle Solaris. La etiqueta predeterminada que está asignada refleja el nivel de confianza adecuado para el host y los usuarios.

Debido a que las comunicaciones con los hosts sin etiquetas se limitan esencialmente a la etiqueta predeterminada, estos hosts también se denominan *hosts de una sola etiqueta*.

Dominio de interpretación en plantillas de seguridad

Las organizaciones que utilizan el mismo dominio de interpretación (DOI) deben acordar entre sí para interpretar la información de la etiqueta y otros atributos de seguridad de la misma manera. Cuando Trusted Extensions realiza una comparación de etiquetas, se efectúa una comprobación para determinar si el DOI es igual.

Un sistema Trusted Extensions aplica la política de etiquetas en un valor DOI. Todas las zonas de un sistema Trusted Extensions deben operar en el mismo DOI. Un sistema Trusted Extensions no proporciona el tratamiento de excepciones en los paquetes que se recibieron de un sistema que utiliza un DOI diferente.

Si el sitio utiliza un valor DOI distinto del predeterminado, debe agregar este valor en el archivo `/etc/system` y cambiar el valor en cada plantilla de seguridad. Para informarse acerca del

procedimiento inicial, consulte "Configure the Domain of Interpretation" de *Trusted Extensions Configuration Guide*. Para configurar el DOI en cada plantilla de seguridad, consulte el Ejemplo 13–1.

Rango de etiquetas en plantillas de seguridad

Los atributos de la etiqueta mínima y la etiqueta máxima se utilizan para establecer el rango de etiquetas para los hosts con etiquetas y sin etiquetas. Estos atributos se utilizan para realizar lo siguiente:

- Establecer el rango de etiquetas que pueden utilizarse cuando se establece la comunicación con un host CIPSO remoto

  Para que se envíe un paquete a un host de destino, la etiqueta del paquete debe estar dentro del rango de etiquetas asignado al host de destino en la plantilla de seguridad para ese host.
- Establecer un rango de etiquetas para los paquetes que se reenvían mediante una puerta de enlace CIPSO o una sin etiquetas

  Puede especificarse el rango de etiquetas en la plantilla para un tipo de host sin etiquetas. El rango de etiquetas activa el host para reenviar los paquetes que no están necesariamente en la etiqueta del host, pero se encuentran dentro de un rango de etiquetas especificado.

Conjunto de etiquetas de seguridad en Security Templates

El conjunto de etiquetas de seguridad define un máximo de cuatro etiquetas discretas en que el host remoto puede aceptar, enviar o reenviar paquetes. Este atributo es opcional. De manera predeterminada, no hay ningún conjunto de etiquetas de seguridad definido.

Mecanismo de reserva de la red de confianza

La base de datos `tnrhdb` puede asignar de manera directa o indirecta una plantilla de seguridad a un host en particular. La asignación directa asigna una plantilla a la dirección IP de un host. Un mecanismo de reserva gestiona la asignación indirecta. En primer lugar, el software de la red de confianza busca una entrada que asigne específicamente la dirección IP del host a una plantilla. Si el software no encuentra una entrada específica para el host, busca el "prefijo más extenso de bits coincidentes". Puede asignar indirectamente un host a una plantilla de seguridad cuando la dirección IP del host está comprendida dentro del "prefijo más extenso de bits coincidentes" de una dirección IP que tiene una longitud de prefijo fija.

En IPv4, puede realizar una asignación indirecta mediante la subred. Cuando se realiza una asignación indirecta con 1, 2, 3 ó 4 octetos de cero (0) final, el software calcula una longitud de prefijo de 24, 16, 8 ó 0, respectivamente. Las entradas 3 – 6 en la Tabla 12–1 muestran este mecanismo de reserva.

También puede determinar una longitud de prefijo fija si agrega una barra diagonal (/) seguida del número de bits fijos. Las direcciones de red IPv4 pueden tener una longitud de prefijo entre 1 y 32. Las direcciones de red IPv6 pueden tener una longitud de prefijo entre 1 y 128.

La siguiente tabla proporciona ejemplos de direcciones de host y de reserva. Si una dirección del conjunto de direcciones de reserva está asignada de manera directa, el mecanismo de reserva no se utiliza para esa dirección.

TABLA 12–1 Entradas del mecanismo de reserva y la dirección de host de `tnrhdb`

Versión de IP	Entrada `tnrhdb`	Direcciones incluidas
IPv4	`192.168.118.57:cipso`	`192.168.118.57`
	`192.168.118.57/32:cipso`	`/32` establece una longitud de prefijo de 32 bits fijos.
	`192.168.118.128/26:cipso`	De `192.168.118.0` a `192.168.118.63`
	`192.168.118.0:cipso`	Todas las direcciones de la red `192.168.118.`
	`192.168.118.0/24:cipso`	
	`192.168.0.0/24:cipso`	Todas las direcciones de la red `192.168.0.`
	`192.168.0.0:cipso`	Todas las direcciones de la red `192.168.`
	`192.168.0.0/16:cipso`	
	`192.0.0.0:cipso`	Todas las direcciones de la red `192.`
	`192.0.0.0/8:cipso`	
	`192.168.0.0/32:cipso`	Dirección de red `192.168.0.0`. (no es una dirección de comodín)
	`192.168.118.0/32:cipso`	Dirección de red `192.168.118.0`. (no es una dirección de comodín)
	`192.0.0.0/32:cipso`	Dirección de red `192.0.0.0`. (no es una dirección de comodín)
	`0.0.0.0/32:cipso`	Dirección de host `0.0.0.0`. (no es una dirección de comodín)
	`0.0.0.0:cipso`	Todas las direcciones de todas las redes.

TABLA 12–1 Entradas del mecanismo de reserva y la dirección de host de tnrhdb *(Continuación)*

Versión de IP	Entrada tnrhdb	Direcciones incluidas
IPv6	2001\:DB8\:22\:5000\:\:21f7:cipso	2001:DB8:22:5000::21f7
	2001\:DB8\:22\:5000\:\:0/52:cipso	De 2001:DB8:22:5000::0 a 2001:DB8:22:5fff:ffff:ffff:ffff:ffff
	0\:\:0/0:cipso	Todas las direcciones de todas las redes.

Observe que la dirección `0.0.0.0/32` coincide con la dirección específica `0.0.0.0`. La entrada `tnrhdb` `0.0.0.0/32:admin_low` resulta útil en un sistema cuya dirección literal, `0.0.0.0`, se usa como una dirección IP de origen. Por ejemplo, los clientes DHCP se contactan con el servidor DHCP como `0.0.0.0` antes de que el servidor les proporcione una dirección IP.

Para crear una entrada `tnrhdb` en un servidor Sun Ray que presta servicio a clientes DHCP, consulte el Ejemplo 13–13. Dado que `0.0.0.0:admin_low` es la entrada de comodín predeterminada, consulte "Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 192 para informarse sobre los temas que debe tener en cuenta antes de eliminar o cambiar este valor predeterminado.

Para obtener más información sobre la longitud de los prefijos en las direcciones IPv4 e IPv6, consulte "Cómo diseñar un esquema de direcciones IPv4 CIDR" de *Administración de Oracle Solaris: servicios IP* y "Descripción general de las direcciones IPv6" de *Administración de Oracle Solaris: servicios IP*.

Descripción general del enrutamiento en Trusted Extensions

En Trusted Extensions, las rutas que unen los hosts de diferentes redes deben preservar la seguridad en cada etapa de la transmisión. Trusted Extensions agrega atributos de seguridad ampliados a los protocolos de enrutamiento en el SO Oracle Solaris. A diferencia del SO Oracle Solaris, esta versión de Trusted Extensions no admite el enrutamiento dinámico. Para obtener detalles sobre la especificación del enrutamiento estático, consulte la opción `-p` de la página del comando man `route(1M)`.

Paquetes de ruta de enrutadores y puertas de enlace. Aquí se utilizan los términos "puerta de enlace" y "enrutador" de manera intercambiable.

En las comunicaciones entre dos hosts de la misma subred, las comprobaciones de acreditaciones se realizan en los puntos finales sólo porque no participan enrutadores. Las comprobaciones de los rangos de etiquetas se llevan a cabo en el origen. Si el host de recepción ejecuta el software Trusted Extensions, las comprobaciones de los rangos de etiquetas también se efectúan en el destino.

Cuando los hosts de origen y de destino se encuentran en subredes diferentes, el paquete se envía desde el host de origen hasta una puerta de enlace. El rango de etiquetas del destino y la

puerta de enlace del primer salto se comprueban en el origen cuando una ruta está seleccionada. La puerta de enlace envía el paquete a la red en que está conectado el host de destino. Es posible que un paquete atraviese varias puertas de enlace antes de llegar al destino.

Conocimientos básicos del enrutamiento

En las puertas de enlace de Trusted Extensions, las comprobaciones de los rangos de etiquetas se llevan a cabo en algunos casos. Un sistema Trusted Extensions que enruta un paquete entre dos hosts sin etiquetas compara la etiqueta predeterminada del host de origen con la etiqueta predeterminada del host de destino. Cuando los hosts sin etiquetas comparten una etiqueta predeterminada, se enruta el paquete.

Cada puerta de enlace mantiene una lista de rutas con todos los destinos. El enrutamiento estándar de Oracle Solaris incluye opciones para optimizar la ruta. Trusted Extensions proporciona software adicional para comprobar los requisitos de seguridad que se aplican a las opciones de ruta. Se omiten las opciones de Oracle Solaris que no cumplen los requisitos de seguridad.

Entradas de la tabla de enrutamiento en Trusted Extensions

Las entradas de la tabla de enrutamiento de Trusted Extensions pueden incorporar atributos de seguridad. Los atributos de seguridad pueden incluir una palabra clave `cipso`. Los atributos de seguridad deben incluir una etiqueta máxima, una etiqueta mínima y un DOI.

En las entradas que no proporcionan atributos de seguridad, se utilizan los atributos de la plantilla de seguridad de la puerta de enlace.

Comprobaciones de acreditaciones de Trusted Extensions

El software Trusted Extensions determina la idoneidad de una ruta por cuestiones de seguridad. El software efectúa una serie de pruebas que se denominan *comprobaciones de acreditaciones* en el host de origen, el host de destino y las puertas de enlace intermedias.

Nota – En la explicación siguiente, la comprobación de acreditación de un rango de etiquetas también implica la comprobación de un conjunto de etiquetas de seguridad.

La comprobación de acreditación controla el rango de etiquetas y la información de la etiqueta CIPSO. Los atributos de seguridad de una ruta se obtienen de la entrada de la tabla de enrutamiento o de la plantilla de seguridad de la puerta de enlace si la entrada no tiene atributos de seguridad.

En las comunicaciones entrantes, el software de Trusted Extensions obtiene etiquetas de los mismos paquetes siempre que sea posible. La obtención de etiquetas de los paquetes sólo es posible cuando los mensajes se envían desde sistemas que admiten etiquetas. Cuando una etiqueta no está disponible en el paquete, se asigna una etiqueta predeterminada al mensaje desde los archivos de las bases de datos de redes de confianza. Estas etiquetas se utilizan posteriormente en las comprobaciones de acreditaciones. Trusted Extensions aplica varias comprobaciones en los mensajes entrantes, salientes y reenviados.

Comprobaciones de acreditaciones del origen

Las siguientes comprobaciones de acreditaciones se realizan en el proceso o la zona de envío:

- En todos los destinos, la etiqueta de los datos debe estar dentro del rango de etiquetas del próximo salto en la ruta, es decir, el primer salto. Además, la etiqueta debe estar incluida en los atributos de seguridad de la puerta de enlace del primer salto.
- En todos los destinos, el DOI de un paquete saliente debe coincidir con el DOI del host de destino. El DOI también debe coincidir con el DOI de todos los saltos de la ruta, incluida la puerta de enlace del primer salto.
- Cuando el host de destino es un host sin etiquetas, debe cumplirse una de las siguientes condiciones:
  - La etiqueta del host de envío debe coincidir con la etiqueta predeterminada del host de destino.
  - El host de envío tiene el privilegio de establecer comunicaciones de etiqueta cruzada, y la etiqueta del remitente domina la etiqueta predeterminada del destino.
  - El host de envío tiene el privilegio de establecer comunicaciones de etiqueta cruzada, y la etiqueta del remitente es `ADMIN_LOW`. Es decir, el remitente realiza el envío desde la zona global.

Nota – Una comprobación del primer salto tiene lugar cuando se envía un mensaje por medio de una puerta de enlace de un host en una red a un host en otra red.

Comprobaciones de acreditaciones de la puerta de enlace

En un sistema de puerta de enlace de Trusted Extensions, se realizan las siguientes comprobaciones de acreditaciones para la puerta de enlace del próximo salto:

- Si el paquete entrante no tiene etiquetas, hereda la etiqueta predeterminada del host de origen de la entrada `tnrhdb`. De lo contrario, el paquete recibe la etiqueta CIPSO indicada.
- Las comprobaciones para el envío de un paquete se efectúan de manera similar a la acreditación de origen:
  - En todos los destinos, la etiqueta de los datos debe estar dentro del rango de etiquetas del próximo salto. Además, la etiqueta debe estar incluida en los atributos de seguridad que corresponden al host del próximo salto.
  - En todos los destinos, el DOI de un paquete saliente debe coincidir con el DOI del host de destino. El DOI también debe coincidir con el DOI del host del próximo salto.
  - La etiqueta de un paquete sin etiquetas debe coincidir con la etiqueta predeterminada del host de destino.
  - La etiqueta de un paquete CIPSO debe estar dentro del rango de etiquetas del host de destino.

Comprobaciones de acreditaciones del destino

Cuando un host de Trusted Extensions recibe datos, el software realiza las siguientes comprobaciones:

- Si el paquete entrante no tiene etiquetas, hereda la etiqueta predeterminada del host de origen de la entrada `tnrhdb`. De lo contrario, el paquete recibe la etiqueta CIPSO indicada.
- La etiqueta y el DOI del paquete deben ser coherentes con la zona de destino o la etiqueta y el DOI del proceso de destino. La única excepción es cuando el proceso realiza la recepción en un puerto de varios niveles. El proceso que recibe puede obtener un paquete si tiene el privilegio de establecer comunicaciones de etiqueta cruzada y se encuentra en la zona global o tiene una etiqueta que domina la etiqueta del paquete.

Administración del enrutamiento en Trusted Extensions

Trusted Extensions admite varios métodos para el enrutamiento de las comunicaciones entre redes. Como administrador de la seguridad, puede configurar las rutas que aplican el grado de seguridad que requiere la política de seguridad del sitio.

Por ejemplo, los sitios pueden restringir las comunicaciones fuera de la red local para una sola etiqueta. Esta etiqueta se aplica a la información disponible públicamente. Las etiquetas como `UNCLASSIFIED` o `PUBLIC` pueden indicar información pública. Para aplicar la restricción, estos sitios asignan una plantilla de una sola etiqueta a la interfaz de red que está conectada a la red externa. Para obtener más detalles sobre TCP/IP y el enrutamiento, consulte lo siguiente:

- “Planificación de enrutadores en la red” de *Administración de Oracle Solaris: servicios IP*
- “Configuración de sistemas en la red local” de *Administración de Oracle Solaris: servicios IP*
- “Tareas de administración principales de TCP/IP (mapa de tareas)” de *Administración de Oracle Solaris: servicios IP*
- “Preparación de la red para el servicio DHCP (mapa de tareas)” de *Administración de Oracle Solaris: servicios IP*

Selección de los enrutadores en Trusted Extensions

Los hosts de Trusted Extensions ofrecen el mayor grado de confianza para los enrutadores. Es posible que otros tipos de enrutadores no reconozcan los atributos de seguridad de Trusted Extensions. Sin ninguna acción administrativa, se pueden enrutar los paquetes mediante enrutadores que no proporcionen protección de seguridad del MAC.

- Los enrutadores CIPSO descartan los paquetes cuando no encuentran el tipo correcto de información en la sección de opciones de IP del paquete. Por ejemplo, un enrutador CIPSO descarta un paquete si no encuentra una opción CIPSO en las opciones de IP cuando la opción es necesaria o cuando el DOI de las opciones de IP no es consistente con la acreditación del destino.
- Es posible configurar otros tipos de enrutadores que no ejecutan el software de Trusted Extensions para transferir los paquetes o descartar aquellos paquetes que incluyan la opción CIPSO. Sólo las puertas de enlace que reconozcan CIPSO, como las que ofrece Trusted Extensions, pueden utilizar el contenido de la opción de IP CIPSO para aplicar el MAC.

A fin de admitir el enrutamiento de confianza, se ampliaron las tablas de enrutamiento de Solaris 10 para incluir los atributos de seguridad de Trusted Extensions. En “Entradas de la tabla de enrutamiento en Trusted Extensions” en la página 174, se describen los atributos. Trusted Extensions admite el enrutamiento estático, en el que el administrador crea manualmente las entradas de la tabla de enrutamiento. Para obtener detalles, consulte la opción `-p` en la página del comando man `route(1M)`.

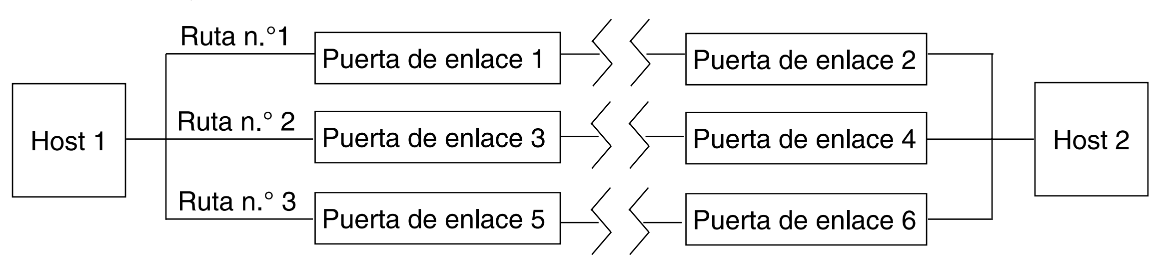
El software de enrutamiento intenta buscar una ruta para el host de destino en las tablas de enrutamiento. Cuando el host no está nombrado de manera explícita, el software de enrutamiento busca una entrada para la subred donde reside el host. Cuando no están definidos ni el host ni la red donde reside el host, el host envía el paquete a una puerta de enlace predeterminada en caso de que esté definida. Se pueden definir varias puertas de enlace predeterminadas, y todas son tratadas del mismo modo.

En esta versión de Trusted Extensions, el administrador de la seguridad configura manualmente las rutas y, a continuación, cambia manualmente la tabla de enrutamiento cuando cambian las condiciones. Por ejemplo, varios sitios tienen una sola puerta de enlace que comunica con el mundo exterior. En estos casos, se puede definir estadísticamente dicha puerta de enlace como *predeterminada* para cada host de la red. Es posible que versiones futuras de Trusted Extensions admitan el encadenamiento dinámico.

Puertas de enlace en Trusted Extensions

A continuación, se muestra un ejemplo de enrutamiento en Trusted Extensions. El diagrama y la tabla muestran tres rutas posibles entre el host 1 y el host 2.

FIGURA 12–1 Rutas y entradas de la tabla de enrutamiento típicas de Trusted Extensions



Ruta	Puerta de enlace del primer salto	Etiqueta mínima	Etiqueta máxima	DOI
N.° 1	Puerta de enlace 1	CONFIDENTIAL	SECRET	1
N.° 2	Puerta de enlace 3	ADMIN_LOW	ADMIN_HIGH	1
N.° 3	Puerta de enlace 5			

- La ruta n.° 1 puede transmitir paquetes dentro del rango de etiquetas de CONFIDENTIAL a SECRET.
- La ruta n.° 2 puede transmitir paquetes de ADMIN_LOW a ADMIN_HIGH.
- La ruta n.° 3 no especifica información del enrutamiento. Por lo tanto, los atributos de seguridad correspondientes se obtienen de la plantilla en la base de datos tnrhtp para la Puerta de enlace 5.

Comandos de enrutamiento en Trusted Extensions

Para mostrar las etiquetas y los atributos de seguridad ampliados para sockets, Trusted Extensions modifica los siguientes comandos de red de Oracle Solaris:

- El comando `netstat -rR` muestra los atributos de seguridad en las entradas de la tabla de enrutamiento.
- El comando `netstat -aR` muestra los atributos de seguridad para sockets.
- El comando `route -p` con las opciones `add` o `delete` cambia las entradas de la tabla de enrutamiento.

Para obtener detalles, consulte las páginas del comando man `netstat`(1M) y `route`(1M).

Para ver ejemplos, consulte "Cómo configurar las rutas con los atributos de seguridad" en la página 196.



CAPÍTULO 13

Gestión de redes en Trusted Extensions (tareas)

En este capítulo se proporcionan detalles y procedimientos de implementación para proteger las redes de Trusted Extensions.

Gestión de la red de confianza (mapa de tareas)

La siguiente tabla hace referencia a los mapas de tareas de procedimientos comunes relativos a las redes de confianza.

Tarea	Descripción	Para obtener instrucciones
Configurar bases de datos de red.	Crear plantillas de hosts remotos y asignar hosts a las plantillas.	"Configuración de bases de datos de red de confianza (mapa de tareas)" en la página 182
Configurar el enrutamiento y revisar las bases de datos de red y la información de red en el núcleo.	Configurar las rutas estáticas que activan los paquetes con etiquetas para que alcancen su destino mediante las puertas de enlace con etiquetas y sin etiquetas. Mostrar el estado de la red.	"Configuración de rutas y comprobación de la información de red en Trusted Extensions (mapa de tareas)" en la página 196
Resolver problemas de redes.	Pasos que se deben seguir para diagnosticar problemas de redes con paquetes con etiquetas.	"Resolución de problemas de la red de confianza (mapa de tareas)" en la página 202

Configuración de bases de datos de red de confianza (mapa de tareas)

El software de Trusted Extensions incluye las bases de datos `tnrhtp` y `tnrhdb`. Estas bases de datos proporcionan etiquetas para los hosts remotos que se contactan con el sistema. Solaris Management Console proporciona la interfaz gráfica de usuario que se utiliza para administrar estas bases de datos.

El siguiente mapa de tareas describe las tareas para crear plantillas de seguridad y aplicarlas a los hosts.

Tarea	Descripción	Para obtener instrucciones
Determinar si el sitio requiere plantillas de seguridad personalizadas.	Evaluar la plantillas existentes según los requisitos de seguridad del sitio.	"Cómo determinar si necesita plantillas de seguridad específicas del sitio" en la página 183
Acceder a la herramienta Security Templates en Solaris Management Console.	Acceder a la herramienta para modificar las bases de datos de red de confianza.	"Cómo abrir las herramientas de redes de confianza" en la página 184
Modificar las plantillas de seguridad.	Cambiar las definiciones de los atributos de seguridad en la red de confianza mediante la modificación de las bases de datos de red de confianza.	"Cómo crear una plantilla de host remoto" en la página 185
	Cambiar el dominio de interpretación a un valor distinto de 1.	Ejemplo 13–1
	Crear una plantilla de seguridad para hosts con etiquetas que restrinja la comunicación entre otros hosts con una sola etiqueta.	Ejemplo 13–2
	Crear una plantilla de seguridad para hosts sin etiquetas que funcionen como puertas de enlace de una sola etiqueta.	Ejemplo 13–3
	Crear una plantilla de seguridad para hosts con un rango de etiquetas restringido.	Ejemplo 13–4
	Crear una plantilla de seguridad para un host que especifique un conjunto de etiquetas discretas en su rango de etiquetas.	Ejemplo 13–5
	Crear una plantilla de seguridad para redes y sistemas sin etiquetas.	Ejemplo 13–6
	Crear una plantilla de seguridad para dos sistemas de desarrolladores.	Ejemplo 13–7

Tarea	Descripción	Para obtener instrucciones
Agregar hosts a la red conocida.	Agregar sistemas y redes a la red de confianza.	"Cómo agregar hosts a la red conocida del sistema" en la página 189
Proporcionar acceso a hosts remotos mediante entradas de comodín.	Permitir que los hosts que se encuentren dentro de un rango dado de direcciones IP se comuniquen con un sistema mediante la asignación indirecta de cada host a la misma plantilla de seguridad.	Ejemplo 13–8 Ejemplo 13–9 Ejemplo 13–10
Cambiar la entrada de comodín `admin_low` en el archivo `tnrhdb`.	Aumentar la seguridad por medio del reemplazo de la entrada de comodín con direcciones específicas con las que los host se contactan en el momento del inicio.	"Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 192
	Aumentar la seguridad por medio del reemplazo de la entrada de comodín con una red de hosts con etiquetas como valor predeterminado.	Ejemplo 13–11
Crear una entrada para la dirección de host `0.0.0.0`	Configurar un servidor Sun Ray para aceptar el contacto inicial desde un cliente remoto	Ejemplo 13–13
Asignar plantillas de seguridad.	Asociar una plantilla con una dirección IP o lista de direcciones IP contiguas.	"Cómo asignar una plantilla de seguridad a un host o a un grupo de hosts" en la página 190

▼ Cómo determinar si necesita plantillas de seguridad específicas del sitio

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 Familiarícese con las plantillas Trusted Extensions.

Lea el archivo `tnrhtp` en un host local. Los comentarios del archivo sirven de ayuda. También puede ver los valores de atributo de seguridad de la herramienta Security Templates de Solaris Management Console.

- Las plantillas predeterminadas coinciden con cualquier instalación. El rango de etiquetas para cada plantilla es de `ADMIN_LOW` a `ADMIN_HIGH`.
- La plantilla `cipso` define un tipo de host CIPSO cuyo dominio de interpretación es `1`. El rango de etiquetas para cada plantilla es de `ADMIN_LOW` a `ADMIN_HIGH`.
- La plantilla de `admin_low` define un host sin etiquetas cuyo dominio de interpretación es `1`. La etiqueta predeterminada de la plantilla es `ADMIN_LOW`. El rango de etiquetas para cada plantilla es de `ADMIN_LOW` a `ADMIN_HIGH`. En la configuración predeterminada, se asigna la

dirección `0.0.0.0` a esta plantilla. Por lo tanto, todos los hosts no CIPSO se tratan como hosts que operan en la etiqueta de seguridad `ADMIN_LOW`.

2 **Mantener las plantillas predeterminadas.**

Por razones de soporte, no suprima ni modifique las plantillas predeterminadas. Puede cambiar el host que se asigna a estas plantillas predeterminadas. Para obtener un ejemplo, consulte "Cómo limitar los hosts que se pueden contactar en la red de confianza" en la página 192.

3 **Cree plantillas nuevas si desea realizar alguna de las siguientes acciones:**

- Limite el rango de etiquetas de un host o un grupo de hosts.
- Crear un host de una sola etiqueta.
- Crear un host que reconozca algunas etiquetas discretas.
- Utilizar un dominio de interpretación diferente de `1`.
- Requiera una etiqueta predeterminada para hosts sin etiquetas que no sea `ADMIN_LOW`.

Para obtener detalles, consulte "Cómo crear una plantilla de host remoto" en la página 185.

▼ Cómo abrir las herramientas de redes de confianza

Antes de empezar Debe estar en la zona global en un rol que pueda modificar la seguridad de la red. Por ejemplo, los roles que tengan asignados los perfiles de derechos de seguridad de la información o de las redes pueden modificar las configuraciones de seguridad. El rol de administrador de la seguridad incluye estos perfiles.

Para utilizar la caja de herramientas LDAP, debe haber completado "Configuring the Solaris Management Console for LDAP (Task Map)" de *Trusted Extensions Configuration Guide*.

1 **Inicie Solaris Management Console.**

Para obtener detalles, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

2 **Utilice la herramienta adecuada.**

- Para modificar una plantilla, utilice la herramienta Security Templates.

  Todas las plantillas que están definidas actualmente se muestran en el panel derecho. Al seleccionar o crear una plantilla, la ayuda en pantalla está disponible en el panel izquierdo.
- Para asignar un host a una plantilla, utilice la herramienta Security Templates.
- Para crear un host que se pueda asignar a una plantilla, utilice la herramienta Computers and Networks.

- Para asignar una etiqueta a una zona, utilice la herramienta Trusted Network Zones. Para obtener más información sobre las zonas en Trusted Extensions, consulte el Capítulo 10, "Gestión de zonas en Trusted Extensions (tareas)".

▼ Cómo crear una plantilla de host remoto

Antes de empezar Debe estar en la zona global en un rol que pueda modificar la seguridad de la red. Por ejemplo, los roles que tengan asignados los perfiles de derechos de seguridad de la información o de las redes pueden modificar las configuraciones de seguridad. El rol de administrador de la seguridad incluye estos perfiles.

1 En Solaris Management Console, vaya a la herramienta Security Templates.

Consulte "Cómo abrir las herramientas de redes de confianza" en la página 184 para conocer los pasos.

2 En Computers and Networks, haga doble clic en Security Templates.

Las plantillas existentes se muestran en el panel View. Estas plantillas describen los atributos de seguridad para los hosts que este sistema puede contactar. Estos hosts incluyen hosts CIPSO que se ejecutan en Trusted Extensions y hosts sin etiquetas.

3 Examine la plantilla de `cipso`.

Vea qué hosts y qué redes ya están asignadas a esta plantilla.

4 Examine la plantilla `admin_low`.

Vea qué hosts y qué redes ya están asignadas a esta plantilla.

5 Cree una plantilla.

Si las plantillas proporcionadas no incluyen una descripción suficiente de los hosts que pueden estar comunicados con este sistema, seleccione Add Template en el menú Action.

Utilice la ayuda en pantalla para obtener asistencia. Antes de asignar hosts a las plantillas, cree todas las plantillas que su sitio requiere.

6 (Opcional) Modifique una plantilla existente que no sea una plantilla predeterminada.

Haga doble clic en la plantilla y utilice la ayuda en pantalla para obtener asistencia. Puede cambiar los hosts asignados o las redes asignadas.

Ejemplo 13–1 Creación de una plantilla de seguridad con un valor de dominio de interpretación diferente

En este ejemplo, la red del administrador de la seguridad tiene un dominio de interpretación cuyo valor es diferente de `1`. El equipo que configuró el sistema al inicio completó "Configure the Domain of Interpretation" de *Trusted Extensions Configuration Guide*.

Primero, el administrador de la seguridad confirma el valor del dominio de interpretación en el archivo/etc/system:

```
# grep doi /etc/system
set default_doi = 4
```

Luego, en la herramienta Security Templates, por cada plantilla que el administrador crea, el valor de doi se establece en 4. El administrador de la seguridad crea la plantilla siguiente para el sistema de una sola etiqueta que se describe en el Ejemplo 13–2:

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 4
min_sl: PUBLIC
max_sl: PUBLIC
```

Ejemplo 13–2 Creación de una plantilla de seguridad que tiene una sola etiqueta

En este ejemplo, el administrador de la seguridad desea crear una puerta de enlace que únicamente pueda transferir paquetes en una sola etiqueta, PUBLIC. Mediante la herramienta Security Templates de Solaris Management Console, el administrador crea una plantilla y asigna el host de la puerta de enlace a la plantilla.

Primero, el host de la puerta de enlace y la dirección IP se agregan a la herramienta Computers and Networks.

```
gateway-1
192.168.131.75
```

Luego, se crea la plantilla en la herramienta Security Templates. Los siguientes son los valores de la plantilla:

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 1
min_sl: PUBLIC
max_sl: PUBLIC
```

La herramienta proporciona el valor hexadecimal para PUBLIC, 0X0002-08-08.

Por último, el host gateway-1 se asigna a la plantilla por su nombre y dirección IP.

```
gateway-1
192.168.131.75
```

En un host local, la entrada tnrhtp se verá similar a la siguiente:

```
cipso_public:host_type=cipso;doi=1;min_sl=0X0002-08-08;max_sl=0X0002-08-08;
```

En un host local, la entrada tnrhdb se verá similar a la siguiente:

```
# gateway-1
192.168.131.75:cipso_public
```

Ejemplo 13–3 Creación de una plantilla de seguridad para un enrutador sin etiquetas

Cualquier enrutador IP puede reenviar los mensajes con etiquetas CIPSO aunque el enrutador no admita etiquetas de manera explícita. Por ejemplo, un enrutador sin etiquetas necesita una etiqueta predeterminada para definir el nivel en el que se deben tratar las conexiones con el enrutador (quizás para la gestión del enrutador). En este ejemplo, el administrador de la seguridad crea un enrutador que puede reenviar tráfico en cualquier etiqueta, pero toda comunicación directa con el enrutador se gestiona en la etiqueta predeterminada, `PUBLIC`.

En Solaris Management Console, el administrador crea una plantilla y asigna el host de la puerta de enlace a la plantilla.

Primero, el enrutador y su dirección IP se agregan a la herramienta Computers and Networks.

```
router-1
192.168.131.82
```

Luego, se crea la plantilla en la herramienta Security Templates. Los valores siguientes figuran en la plantilla:

```
Template Name: UNL_PUBLIC
Host Type: UNLABELED
DOI: 1
Default Label: PUBLIC
Minimum Label: ADMIN_LOW
Maximum Label: ADMIN_HIGH
```

La herramienta proporciona el valor hexadecimal para las etiquetas.

Por último, el enrutador `router-1` se asigna a la plantilla por su nombre y dirección IP.

```
router-1
192.168.131.82
```

Ejemplo 13–4 Creación de una plantilla de seguridad con un rango de etiquetas limitado

En este ejemplo, el administrador de la seguridad desea crear una puerta de enlace que restrinja los paquetes a un rango de etiquetas estrecho. En Solaris Management Console, el administrador crea una plantilla y asigna el host de la puerta de enlace a la plantilla.

Primero, el host y su dirección IP se agregan a la herramienta Computers and Networks.

```
gateway-ir
192.168.131.78
```

Luego, se crea la plantilla en la herramienta Security Templates. Los valores siguientes figuran en la plantilla:

```
Template Name: CIPSO_IUO_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: CONFIDENTIAL : INTERNAL USE ONLY
Maximum Label: CONFIDENTIAL : RESTRICTED
```

La herramienta proporciona el valor hexadecimal para las etiquetas.

Por último, la puerta de enlace `gateway-ir` se asigna a la plantilla por su nombre y dirección IP.

```
gateway-ir
192.168.131.78
```

Ejemplo 13–5 Creación de una plantilla de seguridad con un conjunto de etiquetas de seguridad

En este ejemplo, el administrador de la seguridad desea crear una plantilla de seguridad que reconoce solamente dos etiquetas. En Solaris Management Console, el administrador crea una plantilla y asigna el host de la puerta de enlace a la plantilla.

Primero, se agregan todos los hosts y las direcciones IP que utilizará esta plantilla a la herramienta Computers and Networks.

```
host-slset1
192.168.132.21

host-slset2
192.168.132.22

host-slset3
192.168.132.23

host-slset4
192.168.132.24
```

Luego, se crea la plantilla en la herramienta Security Templates. Los valores siguientes figuran en la plantilla:

```
Template Name: CIPSO_PUB_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: PUBLIC
Maximum Label: CONFIDENTIAL : RESTRICTED
SL Set: PUBLIC, CONFIDENTIAL : RESTRICTED
```

La herramienta proporciona el valor hexadecimal para las etiquetas.

Por último, el rango de direcciones IP se asigna a la plantilla con el botón Wildcard y un prefijo.

```
192.168.132.0/17
```

Ejemplo 13–6 Creación de una plantilla sin etiquetas en la etiqueta PUBLIC

En este ejemplo, el administrador de la seguridad activa una subred de los sistemas Oracle Solaris para que se incluya la etiqueta PUBLIC en la red de confianza. La plantilla tiene los siguientes valores:

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
DOI: 1

Wildcard Entry: 10.10.0.0
Prefix: 16
```

Todos los sistemas de la subred 10.10.0.0 se gestionan en la etiqueta PUBLIC.

Ejemplo 13–7 Creación de una plantilla con etiquetas para desarrolladores

En este ejemplo, el administrador de la seguridad crea una plantilla SANDBOX. Esta plantilla se asigna a los sistemas que utilizan los desarrolladores de software de confianza. Los dos sistemas que tienen asignada esta plantilla crean y prueban los programas con etiquetas. Sin embargo, estas pruebas no afectan a otros sistemas con etiquetas, porque la etiqueta SANDBOX está separada de las otras etiquetas de la red.

```
Template Name: cipso_sandbox
Host Type: CIPSO
Minimum Label: SANDBOX
Maximum Label: SANDBOX
DOI: 1

Hostname: DevMachine1
IP Address: 196.168.129.129

Hostname: DevMachine2
IP Address: 196.168.129.102
```

Los desarrolladores que utilizan estos sistemas pueden comunicarse entre sí en la etiqueta SANDBOX.

▼ Cómo agregar hosts a la red conocida del sistema

La herramienta Computers de Solaris Management Console es idéntica a la herramienta Computers de SO Oracle Solaris. Este procedimiento se proporciona aquí para su comodidad. Después de que se establecen los hosts conocidos, debe asignar los hosts a una plantilla de seguridad.

Antes de empezar Debe estar en un administrador que pueda gestionar redes. Por ejemplo, los roles que incluyen los perfiles de derechos de gestión de red o administración del sistema pueden gestionar redes.

1 En Solaris Management Console, vaya a la herramienta Computers.

Para obtener detalles, consulte "Cómo abrir las herramientas de redes de confianza" en la página 184.

2 En la herramienta Computers, confirme que desea ver todos los equipos de la red.

3 Agregue un host con el que este sistema pueda contactarse.

Debe agregar todos los hosts con los que este sistema pueda contactarse, incluidos todos los enrutadores estáticos y los servidores de auditoría.

a. **En el menú Action, seleccione Add Computer.**

b. **Identifique el host por nombre y dirección IP.**

c. **(Opcional) Proporcione información adicional sobre el host.**

d. **Para agregar el host, haga clic en Apply.**

e. **Cuando las entradas estén completas, haga clic en OK.**

4 Agregue un grupo de hosts con los que este sistema pueda contactarse.

Utilice la ayuda en pantalla para agregar grupos de hosts con una dirección IP de red.

▼ Cómo asignar una plantilla de seguridad a un host o a un grupo de hosts

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

Todos los hosts que desee asignar a una plantilla deben existir en la herramienta Computers and Networks. Para obtener detalles, consulte "Cómo agregar hosts a la red conocida del sistema" en la página 189.

1 En Solaris Management Console, vaya a la herramienta Security Templates.

Para obtener detalles, consulte "Cómo abrir las herramientas de redes de confianza" en la página 184.

2 Haga doble clic en el nombre de plantilla correspondiente.

3 Haga clic en la ficha Hosts Assigned to Template.

4 Para asignar la plantilla a un solo host, realice las siguientes acciones:

a. En el campo Hostname, escriba el nombre del host.

b. En el campo IP Address, escriba la dirección del host.

c. Haga clic en el botón Agregar.

d. Para guardar los cambios, haga clic en OK.

5 Para asignar una plantilla a un grupo de hosts con direcciones contiguas, realice las siguientes acciones:

a. Haga clic en Wildcard.

b. En el campo IP Address, escriba la dirección IP.

c. En el campo Prefix, escriba el prefijo que describe el grupo de las direcciones contiguas.

d. Haga clic en el botón Agregar.

e. Para guardar los cambios, haga clic en OK.

Ejemplo 13–8 Agregación de una red IPv4 como entrada de comodín

En el ejemplo siguiente, un administrador de la seguridad asigna varias subredes IPv4 a la misma plantilla de seguridad. En la ficha Hosts Assigned to Template, el administrador agrega las siguientes entradas de comodín:

```
IP Address: 192.168.113.0
IP address: 192.168.75.0
```

Ejemplo 13–9 Agregación de una lista de hosts IPv4 como entrada de comodín

En el ejemplo siguiente, un administrador de la seguridad asigna direcciones IPv4 contiguas que no están en los límites de octetos de la misma plantilla de seguridad. En la ficha Hosts Assigned to Template, el administrador agrega las siguientes entradas de comodín:

```
IP Address: 192.168.113.100
Prefix Length: 25
```

Esta entrada de comodín cubre el rango de direcciones de `192.168.113.0` a `192.168.113.127`. La dirección incluye `192.168.113.100`.

Ejemplo 13–10 Agregación de una lista de hosts IPv6 como entrada de comodín

En el ejemplo siguiente, un administrador de la seguridad asigna direcciones IPv6 contiguas a la misma plantilla de seguridad. En la ficha Hosts Assigned to Template, el administrador agrega las siguientes entradas de comodín:

```
IP Address: 2001:a08:3903:200::0
Prefix Length: 56
```

Esta entrada de comodín cubre el rango de direcciones de `2001:a08:3903:200::0` a `2001:a08:3903:2ff:ffff:ffff:ffff:ffff`. La dirección incluye `2001:a08:3903:201:20e:cff:fe08:58c`.

▼ Cómo limitar los hosts que se pueden contactar en la red de confianza

Este procedimiento protege los hosts con etiquetas del contacto de hosts sin etiquetas arbitrarios. Si Trusted Extensions está instalado, esta plantilla predeterminada define cada host en la red. Utilice este procedimiento para enumerar hosts sin etiquetas específicos.

El archivo local `tnrhdb` de cada sistema se utiliza para contactar con la red en el momento del inicio. De manera predeterminada, cada host que no se proporciona con una plantilla CIPSO se define mediante la plantilla `admin_low`. Esta plantilla asigna todos los sistemas que no estén definidos de ningún otro modo (`0.0.0.0`) como sistemas sin etiquetas con la etiqueta predeterminada `admin_low`.



Precaución – La plantilla predeterminada `admin_low` puede ser un riesgo de seguridad en una red de Trusted Extensions. Si la seguridad del sitio requiere una protección elevada, el administrador de la seguridad puede eliminar la entrada de comodín `0.0.0.0` después de que se instala el sistema. La entrada debe reemplazarse con entradas para cada host con el que el sistema se contacta durante el inicio.

Por ejemplo, los servidores DNS, los servidores del directorio principal, los servidores de auditoría, las direcciones de difusión y multidifusión, y los enrutadores deben estar en el archivo local `tnrhdb` uva vez que se elimine la entrada de comodín `0.0.0.0`.

Si, al inicio, una aplicación reconoce clientes en la dirección de host `0.0.0.0`, debe agregar la entrada de host `0.0.0.0/32:admin_low` a la base de datos `tnrhdb`. Por ejemplo, para recibir las solicitudes de conexión inicial de los posibles clientes Sun Ray, los servidores Sun Ray deben incluir esta entrada. A continuación, cuando el servidor reconoce los clientes, se proporciona una dirección IP a los clientes y se los conecta como clientes CIPSO.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

Todos los hosts que se deben contactar en el momento del inicio deben existir en la herramienta Computers and Networks.

1 **En Solaris Management Console, vaya a la herramienta Security Templates en el ámbito Files.**

El ámbito Files protege el sistema durante el inicio. Para acceder a la herramienta Security Templates, consulte "Cómo abrir las herramientas de redes de confianza" en la página 184.

2 **Modifique los hosts que se asignan a la plantilla `admin_low`.**

a. **Haga doble clic en la plantilla `admin_low`.**

Cada host que se agrega se puede contactar durante el inicio en la etiqueta `ADMIN_LOW`.

b. **Haga clic en la ficha Hosts Assigned to Template.**

Cada host que se agrega se puede contactar durante el inicio en la etiqueta `ADMIN_LOW`.

c. **Agregue cada host sin etiquetas que se deba contactar en el momento del inicio.**

Para obtener detalles, consulte "Cómo asignar una plantilla de seguridad a un host o a un grupo de hosts" en la página 190.

Incluya cada enrutador "on-link" que no esté ejecutando Trusted Extensions, mediante el cual este host debe comunicarse.

d. **Agregue los rangos de los hosts que se deben contactar en el momento del inicio.**

e. **Elimine la entrada `0.0.0.0`.**

3 **Modifique los hosts que se asignan a la plantilla `cipso`.**

a. **Haga doble clic en la plantilla `cipso`.**

Cada host que se agrega se puede contactar durante el inicio.

b. **Haga clic en la ficha Hosts Assigned to Template.**

Cada host que se agrega se puede contactar durante el inicio en la etiqueta `ADMIN_LOW`.

c. **Agregue cada host con etiquetas con el que se debe establecer contacto durante el inicio.**

Para obtener detalles, consulte "Cómo asignar una plantilla de seguridad a un host o a un grupo de hosts" en la página 190.

- Incluya el servidor LDAP.
- Incluya cada enrutador "on-link" que esté ejecutando Trusted Extensions, mediante el cual este host debe comunicarse.
- Asegúrese de que todas las interfaces de red estén asignadas a la plantilla.
- Incluya las direcciones de difusión.

d. **Agregue los rangos de los hosts que se deben contactar en el momento del inicio.**

4 **Compruebe que las asignaciones de hosts permitan que el sistema se inicie.**

Ejemplo 13–11 Cambio de la etiqueta de la entrada 0.0.0.0 `tnrhdb`

En este ejemplo, el administrador de la seguridad crea un sistema de puerta de enlace pública. El administrador elimina la entrada `0.0.0.0` de la plantilla `admin_low` y asigna la entrada a una plantilla sin etiquetas que se denomina `public`. El sistema reconoce cualquier sistema que no figure en su archivo `tnrhdb` como sistema sin etiquetas con los atributos de seguridad de la plantilla de seguridad `public`.

A continuación se describe una plantilla sin etiquetas creada específicamente para puertas de enlace públicas.

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
DOI: 1
```

Ejemplo 13–12 Enumeración de equipos que se deben contactar durante el inicio en la base de datos `tnrhdb`

El siguiente ejemplo muestra la base de datos local `tnrhdb` con entradas para un cliente LDAP con dos interfaces de red. El cliente se comunica con otra red y con los enrutadores.

```
127.0.0.1:cipso              Loopback address
192.168.112.111:cipso        Interface 1 of this host
192.168.113.111:cipso        Interface 2 of this host
10.6.6.2:cipso               LDAP server
192.168.113.6:cipso          Audit server
192.168.112.255:cipso        Subnet broadcast address
192.168.113.255:cipso        Subnet broadcast address
192.168.113.1:cipso          Router
192.168.117.0:cipso          Another Trusted Extensions network
192.168.112.12:public        Specific network router
192.168.113.12:public        Specific network router
224.0.0.2:public             Multicast address
255.255.255.255:admin_low        Broadcast address
```

Ejemplo 13–13 Establecimiento de la dirección de host 0.0.0.0 como entrada `tnrhdb` válida

En este ejemplo, el administrador de la seguridad configura un servidor Sun Ray para que acepte las solicitudes de conexión inicial de clientes potenciales. El servidor usa una topología privada y los valores predeterminados:

```
# utadm -a bge0
```

Primero, el administrador determina el nombre de dominio de Solaris Management Console:

```
SMCserver # /usr/sadm/bin/dtsetup scopes
Getting list of managable scopes...
Scope 1 file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM
```

Luego, el administrador agrega la entrada para la conexión inicial del cliente con la base de datos `tnrhdb` del servidor Sun Ray. Mientras el administrador está probando, la dirección de comodín predeterminada se sigue utilizando para todas las direcciones desconocidas:

```
SunRayServer # /usr/sadm/bin/smtnrhdb \
add -D file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM \
-- -w 0.0.0.0 -p 32 -n admin_low
Authenticating as user: root

Please enter a string value for: password ::
... from machine1.ExampleCo.COM was successful.
```

Después de que se ejecuta este comando, aparece una base de datos `tnrhdb` similar a la siguiente. El resultado del comando `smtnrhdb` aparece resaltado:

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## Default wildcard address
0.0.0.0:admin_low
    Other addresses to be contacted at boot

# tnchkdb -h /etc/security/tsol/tnrhdb
```

Después de que esta fase de la prueba se realizó correctamente, el administrador elimina la dirección de comodín predeterminada a fin de hacer la configuración más segura, comprueba la sintaxis de la base de datos `tnrhdb` y vuelve a realizar la prueba. La base de datos `tnrhdb` final será similar a la siguiente:

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## 0.0.0.0:admin_low - no other systems can enter network at admin_low
    Other addresses to be contacted at boot
```

Configuración de rutas y comprobación de la información de red en Trusted Extensions (mapa de tareas)

El siguiente mapa de tareas describe las tareas que se realizan para configurar la red y verificar la configuración.

Tarea	Descripción	Para obtener instrucciones
Configurar rutas estáticas.	Describir manualmente la mejor ruta de un host a otro host.	"Cómo configurar las rutas con los atributos de seguridad" en la página 196
Comprobar la precisión de las bases de datos de redes locales.	Utilizar el comando `tnchkdb` para comprobar la validez de la sintaxis de las bases de datos de redes locales.	"Cómo comprobar la sintaxis de las bases de datos de red de confianza" en la página 198
Comparar las entradas de la base de datos de red con las entradas de la caché del núcleo.	Utilizar el comando `tninfo` a fin de determinar si la caché del núcleo se actualizó con la última información de la base de datos.	"Cómo comparar la información de la base de datos de red de confianza con la caché del núcleo" en la página 198
Sincronizar la caché del núcleo con las bases de datos de redes.	Utilizar el comando `tnctl` para actualizar la caché del núcleo con información actualizada de la base de datos de red en un sistema que se esté ejecutando.	"Cómo sincronizar la caché del núcleo con las bases de datos de red de confianza" en la página 200

▼ Cómo configurar las rutas con los atributos de seguridad

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Agregue todas las puertas de enlace y los host de destino que esté utilizando para enrutar paquetes en la red de confianza.**

   Las direcciones se agregan al archivo `/etc/hosts` local o a su equivalente en el servidor LDAP. Utilice la herramienta Computers and Networks de Solaris Management Console. El ámbito Files modifica el archivo `/etc/hosts`. El ámbito LDAP modifica las entradas en el servidor LDAP. Para obtener detalles, consulte "Cómo agregar hosts a la red conocida del sistema" en la página 189.

2. **Asigne cada red, puerta de enlace y host de destino a una plantilla de seguridad.**

   Las direcciones se agregan al archivo `/etc/security/tsol/tnrhdb` o a su equivalente en el servidor LDAP. Utilice la herramienta Security Templates de Solaris Management Console. Para obtener detalles, consulte "Cómo asignar una plantilla de seguridad a un host o a un grupo de hosts" en la página 190.

3 Configure las rutas.

En una ventana de terminal, utilice el comando `route add` para especificar las rutas.

La primera entrada configura una ruta predeterminada. La entrada especifica una dirección de puerta de enlace (`192.168.113.1`) para utilizar cuando no hay una ruta específica definida para el host o el destino del paquete.

```
# route add default 192.168.113.1  -static
```

Para obtener detalles, consulte la página del comando man `route`(1M).

4 Configure una o más entradas de red.

Utilice el indicador `-secattr` para especificar los atributos de seguridad.

En la siguiente lista de comandos, la segunda línea muestra una entrada de red. La tercera línea muestra una entrada de red con un rango de etiquetas de `PUBLIC` a `CONFIDENTIAL : INTERNAL USE ONLY`.

```
# route add default 192.168.113.36
# route add -net 192.168.102.0 gateway-101
# route add -net 192.168.101.0 gateway-102 \
-secattr min_sl=“PUBLIC”,max_sl=”CONFIDENTIAL : INTERNAL USE ONLY”,doi=1
```

5 Configure una o más entradas de host.

La cuarta línea nueva muestra una entrada para el host de una sola etiqueta, `gateway-pub`. `gateway-pub` tiene un rango de etiquetas de `PUBLIC` a `PUBLIC`.

```
# route add default 192.168.113.36
# route add -net 192.168.102.0 gateway-101
# route add -net 192.168.101.0 gateway-102 \
-secattr min_sl="PUBLIC",max_sl="CONFIDENTIAL : INTERNAL USE ONLY",doi=1
# route add -host 192.168.101.3 gateway-pub \
-secattr min_sl="PUBLIC",max_sl="PUBLIC",doi=1
```

Ejemplo 13–14 Agregación de una ruta con un rango de etiquetas de CONFIDENTIAL : INTERNAL USE ONLY a CONFIDENTIAL : RESTRICTED

El siguiente comando `route` agrega a la tabla de enrutamiento los hosts de `192.168.115.0` con `192.168.118.39` como puerta de enlace. El rango de etiquetas es de `CONFIDENTIAL : INTERNAL USE ONLY` a `CONFIDENTIAL : RESTRICTED` y el dominio de interpretación es `1`.

```
$ route add -net 192.168.115.0 192.168.118.39 \
-secattr min_sl="CONFIDENTIAL : INTERNAL USE ONLY",max_sl="CONFIDENTIAL : RESTRICTED",doi=1
```

El resultado de los hosts agregados se muestra con el comando `netstat -rR`. En el fragmento siguiente, se reemplazan otras rutas por puntos suspensivos (...).

```
$ netstat -rRn
...
192.168.115.0        192.168.118.39        UG       0      0
        min_sl=CNF : INTERNAL USE ONLY,max_sl=CNF : RESTRICTED,DOI=1,CIPSO
...
```

▼ Cómo comprobar la sintaxis de las bases de datos de red de confianza

El comando `tnchkdb` comprueba que la sintaxis de cada base de datos de la red sea precisa. Solaris Management Console ejecuta este comando automáticamente cuando se usan las herramientas Security Templates o Trusted Network Zones. En general, debe ejecutar este comando para comprobar la sintaxis de los archivos de las bases de datos que esté configurando para que se usen en el futuro.

Antes de empezar Debe estar en la zona global, en un rol que pueda verificar la configuración de la red. El rol de administrador de la seguridad y el rol de administrador del sistema pueden verificar esta configuración.

- **En una ventana de terminal, ejecute el comando `tnchkdb`.**

```
$ tnchkdb [-h tnrhdb-path] [-t tnrhtp-path] [-z tnzonecfg-path]
checking /etc/security/tsol/tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

Ejemplo 13–15 Comprobación de la sintaxis de una base de datos de red de prueba

En este ejemplo, el administrador de la seguridad prueba un archivo de base de datos de red para su posible uso. Primero, el administrador usa la opción incorrecta. Los resultados de la comprobación se imprimen en la línea para el archivo `tnrhdb`:

```
$ tnchkdb -h /opt/secfiles/trial.tnrhtp
checking /etc/security/tsol/tnrhtp ...
checking /opt/secfiles/trial.tnrhtp ...
line 12: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
line 14: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
checking /etc/security/tsol/tnzonecfg ...
```

Cuando el administrador de la seguridad comprueba el archivo con la opción `-t`, el comando confirma que la sintaxis de la base de datos de prueba `tnrhtp` sea precisa:

```
$ tnchkdb -t /opt/secfiles/trial.tnrhtp
checking /opt/secfiles/trial.tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

▼ Cómo comparar la información de la base de datos de red de confianza con la caché del núcleo

Las bases de datos de red pueden contener información que no se encuentre en la caché del núcleo. Con este procedimiento se comprueba que la información sea idéntica. Cuando usa

Solaris Management Console para actualizar la red, la caché del núcleo se actualiza con la información de la base de datos de la red. El comando `tninfo` resulta útil para la comprobación y la depuración.

Antes de empezar Debe estar en la zona global, en un rol que pueda verificar la configuración de la red. El rol de administrador de la seguridad y el rol de administrador del sistema pueden verificar esta configuración.

● **En una ventana de terminal, ejecute el comando `tninfo`.**

- `tninfo -h` *hostname* muestra la dirección IP y plantilla para el host especificado.
- `tninfo -t` *templatename* muestra la siguiente información:

```
template: template-name
host_type: either CIPSO or UNLABELED
doi: 1
min_sl: minimum-label
hex: minimum-hex-label
max_sl: maximum-label
hex:maximum-hex-label
```

- `tninfo -m` *zone-name* muestra la configuración del puerto de varios niveles (MLP) de una zona.

Ejemplo 13–16 Visualización de puertos de varios niveles en un host

En este ejemplo, se configura un sistema con varias zonas con etiquetas. Todas las zonas comparten la misma dirección IP. Algunas zonas también se configuran con direcciones específicas de las zonas. En esta configuración, el puerto TCP para navegar por la web (puerto `8080`), es un puerto de varios niveles en una interfaz compartida en la zona public. El administrador también configuró `telnet` (puerto TCP `23`) para que sea un puerto de varios niveles en la zona public. Dado que estos dos puertos de varios niveles están en una interfaz compartida, ninguna otra zona, ni siquiera la zona global, puede recibir paquetes de la interfaz compartida en los puertos `8080` y `23`.

Además, el puerto TCP para `ssh` (puerto `22`) es un puerto de varios niveles por zona en la zona public. El servicio de la zona public `ssh` puede recibir cualquier paquete en su dirección específica de la zona dentro del rango de etiquetas de la etiqueta.

El siguiente comando muestra los puertos de varios niveles para la zona public:

```
$ tninfo -m public
private: 22/tcp
shared:  23/tcp;8080/tcp
```

El siguiente comando muestra los puertos de varios niveles para la zona global. Tenga en cuenta que los puertos `23` y `8080` no pueden ser puertos de varios niveles en la zona global porque dicha zona comparte la misma dirección con la zona public:

```
$ tninfo -m global
private: 111/tcp;111/udp;514/tcp;515/tcp;631/tcp;2049/tcp;
         6000-6003/tcp;38672/tcp;60770/tcp;
shared:  6000-6003/tcp
```

▼ Cómo sincronizar la caché del núcleo con las bases de datos de red de confianza

Si el núcleo no se actualizó con la información de la base de datos de red de confianza, existen varias maneras de actualizar la caché del núcleo. Solaris Management Console ejecuta este comando automáticamente cuando se usan las herramientas Security Templates o Trusted Network Zones.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **Para sincronizar la caché del núcleo con las bases de datos de la red, ejecute uno de los siguientes comandos:**

  - **Reinicie el servicio `tnctl`.**

    Precaución – No utilice este método en los sistemas que obtienen la información de las bases de datos de red de confianza desde un servidor LDAP. La información de la base de datos local sobrescribe la información que se obtiene del servidor LDAP.

    ```
    $ svcadm restart  svc:/network/tnctl
    ```

    Este comando lee toda la información de las bases de datos de red de confianza locales en el núcleo.

  - **Actualice la caché del núcleo para las entradas que se hayan agregado recientemente.**

    `$ tnctl -h` *hostname*

    Este comando lee solamente la información desde la opción seleccionada en el núcleo. Para obtener detalles sobre las opciones, consulte el Ejemplo 13–17 y la página del comando man `tnctl`(1M).

  - **Modifique el servicio `tnd`.**

    Nota – El servicio `tnd` se ejecuta solamente si el servicio `ldap` también se ejecuta.

- **Cambie el intervalo de sondeo `tnd`.**

  Esto no actualiza la caché del núcleo. Sin embargo, puede acortar el intervalo de sondeo para actualizar la caché del núcleo con más frecuencia. Para obtener detalles, consulte el ejemplo de la página del comando man `tnd`(1M).

- **Actualice el `tnd`.**

  Este comando de la Utilidad de gestión de servicios (SMF) inicia una actualización inmediata del núcleo con los cambios recientes en las bases de datos de red de confianza.

  ```
  $ svcadm refresh svc:/network/tnd
  ```

- **Reinicie el `tnd` con SMF.**

  ```
  $ svcadm restart svc:/network/tnd
  ```



Precaución – Evite la ejecución del comando `tnd` para reiniciar el `tnd`. Este comando puede interrumpir comunicaciones que se estén realizando con éxito.

Ejemplo 13–17 Actualización del núcleo con las últimas entradas `tnrhdb`

En este ejemplo, el administrador agrega tres direcciones a la base de datos local `tnrhdb`. Primero, el administrador elimina la entrada de comodín `0.0.0.0`.

```
$ tnctl -d -h 0.0.0.0:admin_low
```

Luego, el administrador ve el formato las tres últimas entradas en la base de datos `/etc/security/tsol/tnrhdb`:

```
$ tail /etc/security/tsol/tnrhdb
#\:\:0:admin_low
127.0.0.1:cipso
#\:\:1:cipso
192.168.103.5:admin_low
192.168.103.0:cipso
0.0.0.0/32:admin_low
```

A continuación, el administrador actualiza la caché del núcleo:

```
$ tnctl -h 192.168.103.5
tnctl -h 192.168.103.0
tnctl -h 0.0.0.0/32
```

Por último, el administrador verifica que la caché del núcleo se haya actualizado. La salida de la primera entrada será similar a la siguiente:

```
$ tninfo -h 192.168.103.5
IP Address: 192.168.103.5
Template: admin_low
```

Ejemplo 13–18 Actualización de la información de la red en el núcleo

En este ejemplo, el administrador actualiza la red de confianza con un servidor de impresión público y, luego, comprueba que la configuración del núcleo sea correcta.

```
$ tnctl -h public-print-server
$ tninfo -h public-print-server
IP Address: 192.168.103.55
Template: PublicOnly
$ tninfo -t PublicOnly
==================================
Remote Host Template Table Entries
----------------------------------
template: PublicOnly
host_type: CIPSO
doi: 1
min_sl: PUBLIC
hex: 0x0002-08-08
max_sl: PUBLIC
hex: 0x0002-08-08
```

Resolución de problemas de la red de confianza (mapa de tareas)

El siguiente mapa de tareas describe las tareas que se deben realizar para depurar la red.

Tarea	Descripción	Para obtener instrucciones
Determinar por qué dos hosts no se pueden comunicar.	Se comprueba que las interfaces de un solo sistema estén activas.	"Cómo verificar que las interfaces del host estén activas" en la página 202
	Utilizar las herramientas de depuración cuando dos hosts no se pueden comunicar entre sí.	"Cómo depurar la red de Trusted Extensions" en la página 203
Determinar por qué un cliente LDAP no puede acceder al servidor LDAP.	Se resuelven los problemas de pérdida de conexión entre un servidor LDAP y un cliente.	"Cómo depurar una conexión de cliente con el servidor LDAP" en la página 206

▼ Cómo verificar que las interfaces del host estén activas

Utilice este procedimiento si el sistema no se comunica con otros hosts según lo esperado.

Antes de empezar Debe estar en la zona global, en un rol que pueda verificar la configuración de la red. El rol de administrador de la seguridad y el rol de administrador del sistema pueden verificar esta configuración.

1 **Verifique que la interfaz de la red del sistema esté activa.**

La siguiente salida muestra que el sistema tiene dos interfaces de red: `hme0` y `hme0:3`. Ninguna interfaz está activa.

```
# ifconfig -a
...
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.11 netmask ffffff00 broadcast 192.168.0.255
hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.12 netmask ffffff00 broadcast 192.168.0.255
```

2 **Si la interfaz no está activa, actívela, y luego verifique que haya quedado activada.**

La siguiente salida muestra que ambas interfaces están activas.

```
# ifconfig hme0 up
# ifconfig -a
...
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,...
hme0:3 flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,..
```

▼ Cómo depurar la red de Trusted Extensions

Para depurar dos hosts que deben comunicarse, pero no lo hacen, puede utilizar las herramientas de depuración de Trusted Extensions y Solaris. Por ejemplo, los comandos de depuración de redes de Oracle Solaris, como `snoop` y `netstat`, se encuentran disponibles. Para obtener detalles, consulte las páginas del comando man `snoop`(1M) y `netstat`(1M). Para obtener información sobre los comandos específicos de Trusted Extensions, consulte la Tabla 2–4.

- Para obtener información sobre los problemas para contactarse con zonas con etiquetas, consulte "Gestión de zonas (mapa de tareas)" en la página 130.
- Para obtener información sobre la depuración de los montajes de NFS, consulte "Cómo resolver problemas por fallos de montaje en Trusted Extensions" en la página 160.
- Para obtener información sobre la depuración de las comunicaciones LDAP, consulte "Cómo depurar una conexión de cliente con el servidor LDAP" en la página 206.

Antes de empezar Debe estar en la zona global, en un rol que pueda verificar la configuración de la red. El rol de administrador de la seguridad o el rol de administrador del sistema pueden verificar esta configuración.

1 **Para resolver el problema del daemon de `tnd`, cambie el intervalo de sondeo y recopile la información de depuración.**

Nota – El servicio `tnd` se ejecuta solamente si el servicio `ldap` también se ejecuta.

Para obtener detalles, consulte la página del comando man `tnd`(1M).

2 Compruebe que los hosts que no pueden comunicarse estén utilizando el mismo servicio de nombres.

a. En cada host, revise el archivo `nsswitch.conf`.

i. Verifique los valores de las bases de datos de Trusted Extensions en el archivo `nsswitch.conf`.

Por ejemplo, en un sitio que utiliza LDAP para administrar la red, las entradas son similares a las siguientes:

```
# Trusted Extensions
tnrhtp: files ldap
tnrhdb: files ldap
```

ii. Si los valores son diferentes, corrija el archivo `nsswitch.conf`.

Para modificar estas entradas, el administrador del sistema utiliza la acción Name Service Switch. Para obtener detalles, consulte "Cómo iniciar acciones administrativas de CDE en Trusted Extensions" en la página 56. Esta acción mantiene los permisos de los archivos DAC y MAC necesarios.

b. Compruebe que el servicio de nombres LDAP esté configurado.

```
$ ldaplist -l
```

c. Compruebe que los dos hosts se encuentren en el servicio de nombres LDAP.

```
$ ldaplist -l hosts | grep hostname
```

3 Compruebe que cada host se haya definido correctamente.

a. Utilice la Solaris Management Console para verificar las definiciones.

- En la herramienta Security Templates, compruebe que cada host esté asignado a una plantilla de seguridad que sea compatible con la plantilla de seguridad de los otros host.
- Para un sistema sin etiquetas, compruebe que la asignación de etiquetas predeterminadas sea correcta.
- En la herramienta Trusted Network Zones, compruebe que los puertos de varios niveles (MLP) estén configurados correctamente.

b. Utilice la línea de comandos para comprobar que la información de la red del núcleo sea actual.

Compruebe que la asignación en la caché del núcleo de cada host coincida con la asignación en la red y en el otro host.

Para obtener información de seguridad para hosts de puerta de enlace, origen y destino en la transmisión, utilice el comando `tninfo`.

- **Visualice la dirección IP y la plantilla de seguridad asignada para un host determinado.**

  ```
  $ tninfo -h hostname
  IP Address: IP-address
  Template: template-name
  ```

- **Visualice una definición de la plantilla.**

  ```
  $ tninfo -t template-name
  template: template-name
  host_type: one of CIPSO or UNLABELED
  doi: 1
  min_sl: minimum-label
  hex: minimum-hex-label
  max_sl: maximum-label
  hex: maximum-hex-label
  ```

- **Visualice los puertos de varios niveles para una zona.**

  ```
  $ tninfo -m zone-name
  private: ports-that-are-specific-to-this-zone-only
  shared: ports-that-the-zone-shares-with-other-zones
  ```

4 Corrija cualquier información incorrecta.

- Para cambiar o verificar la información de seguridad de la red, utilice las herramientas de Solaris Management Console. Para obtener detalles, consulte “Cómo abrir las herramientas de redes de confianza” en la página 184
- Para actualizar la caché del núcleo, reinicie el servicio `tnctl` en el host cuya información se encuentre desactualizada. Deje pasar un tiempo hasta que el proceso se complete. Luego, actualice el servicio `tnd`. Si la actualización falla, intente reiniciar el servicio `tnd`. Para obtener detalles, consulte “Cómo sincronizar la caché del núcleo con las bases de datos de red de confianza” en la página 200.

Nota – El servicio `tnd` se ejecuta solamente si el servicio `ldap` también se ejecuta.

Si se reinicia, se borra la caché del núcleo. Durante el inicio, la caché se rellena con información de la base de datos. El archivo `nsswitch.conf` determina si las bases de datos locales o las bases de datos LDAP se utilizan para rellenar el núcleo.

5 Recopile información de la transmisión para usarla como ayuda en la depuración.

- **Verifique la configuración de enrutamiento.**

  Utilice el subcomando `get` hacia el comando `route`.

  ```
  $ route get [ip] -secattr sl=label,doi=integer
  ```

Para obtener detalles, consulte la página del comando man route(1M).

- **Vea la información de la etiqueta en los paquetes.**

  Utilice el comando `snoop -v`.

  La opción `-v` muestra los detalles de los encabezados de los paquetes, incluida la información de la etiqueta. Dado que este comando proporciona información muy detallada, quizás desee restringir los paquetes que el comando examina. Para obtener detalles, consulte la página del comando man snoop(1M).

- **Vea las entradas de la tabla de enrutamiento y los atributos de seguridad en sockets.**

  Utilice la opción `-R` con el comando `netstat -a|-r`.

  La opción `-aR` muestra los atributos de seguridad ampliados para sockets. La opción `-rR` muestra las entradas de la tabla de enrutamiento. Para obtener detalles, consulte la página del comando man netstat(1M).

▼ Cómo depurar una conexión de cliente con el servidor LDAP

Un error en la configuración de la entrada del cliente en el servidor LDAP puede impedir la comunicación del cliente con el servidor. Un error en la configuración de los archivos del cliente también puede impedir la comunicación. Compruebe las entradas y los archivos siguientes cuando intente depurar un problema de comunicación entre el cliente y el servidor.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global del cliente LDAP.

1 **Compruebe que la plantilla del host remoto para el servidor LDAP y para la puerta de enlace con el servidor LDAP sea correcta.**

```
# tninfo -h LDAP-server
# route get LDAP-server
# tninfo -h gateway-to-LDAP-server
```

Si la asignación de una plantilla a un host remoto es incorrecta, asigne el host a la plantilla correcta mediante la herramienta Security Templates de Solaris Management Console.

2 **Revise y corrija el archivo `/etc/hosts`.**

El sistema, las interfaces para las zonas con etiquetas del sistema, la puerta de enlace con el servidor LDAP y el servidor LDAP deben figurar en el archivo. Puede que tenga más entradas.

Busque las entradas duplicadas. Elimine cualquier entrada que sea una zona con etiquetas en otros sistemas. Por ejemplo, si el nombre de su servidor LDAP es `Lserver`, y `LServer-zones` es la interfaz compartida para las zonas con etiquetas, elimine `LServer-zones` de `/etc/hosts`.

3 Si usa DNS, revise y corrija las entradas del archivo `resolv.conf`.

```
# more resolv.conf
search list of domains
domain domain-name
nameserver IP-address

...
nameserver IP-address
```

4 Compruebe que las entradas `tnrhdb` y `tnrhtp` del archivo `nsswitch.conf` sean precisas.

5 Compruebe que el cliente esté configurado correctamente en el servidor.

```
# ldaplist -l tnrhdb client-IP-address
```

6 Compruebe que las interfaces para sus zonas con etiquetas estén configuradas correctamente en el servidor LDAP.

```
# ldaplist -l tnrhdb client-zone-IP-address
```

7 Compruebe que puede aplicar `ping` en el servidor LDAP desde todas las zonas que se encuentran en ejecución.

```
# ldapclient list
...
NS_LDAP_SERVERS= LDAP-server-address
# zlogin zone-name1 ping LDAP-server-address
LDAP-server-address is alive
# zlogin zone-name2 ping LDAP-server-address
LDAP-server-address is alive
...
```

8 Configure LDAP y reinicie el sistema.

a. Para conocer el procedimiento, consulte "Make the Global Zone an LDAP Client in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

b. En cada zona con etiquetas, vuelva a establecer la zona como cliente del servidor LDAP.

```
# zlogin zone-name1
# ldapclient init \
-a profileName=profileName \
-a domainName=domain \
-a proxyDN=proxyDN \
-a proxyPassword=password LDAP-Server-IP-Address
# exit
# zlogin zone-name2 ...
```

c. **Detenga todas las zonas, bloquee los sistemas de archivos y reinicie.**

Si está utilizando ZFS de Oracle Solaris, detenga las zonas y bloquee los sistemas de archivos antes de reiniciar. Si no está utilizando ZFS, puede reiniciar sin detener las zonas y ni bloquear los sistemas de archivos.

```
# zoneadm list
# zoneadm -z zone-name halt
# lockfs -fa
# reboot
```

CAPÍTULO 14

Correo de varios niveles en Trusted Extensions (descripción general)

En este capítulo se tratan la seguridad y los servicios de envío de correo de varios niveles de los sistemas que se configuran con Trusted Extensions.

Servicio de correo de varios niveles

Trusted Extensions proporciona correo de varios niveles para cualquier aplicación de correo. Cuando los usuarios comunes inician su aplicación de correo, la aplicación se abre en la etiqueta actual del usuario. Si los usuarios operan en un sistema de varios niveles, quizás deseen enlazar o copiar sus archivos de inicialización de la aplicación de correo. Para obtener detalles, consulte "Cómo configurar los archivos de inicio para los usuarios en Trusted Extensions" en la página 90.

Funciones de correo de Trusted Extensions

En Trusted Extensions, el rol de administrador del sistema configura y administra servidores de correo según las instrucciones de Oracle Solaris que figuran en la *Guía de administración del sistema: Administración avanzada* y *Administración de Oracle Solaris: servicios IP*. Además, el administrador de la seguridad determina cómo se deben configurar las funciones de correo de Trusted Extensions.

Los siguientes aspectos de la gestión de correo son específicos de Trusted Extensions:

- El archivo `.mailrc` se encuentra en una etiqueta mínima del usuario.

  Por lo tanto, los usuarios que trabajan en varias etiquetas no tienen un archivo `.mailrc` en las etiquetas superiores, a menos que copien o enlacen el archivo `.mailrc` ubicado en el directorio de la etiqueta mínima a cada directorio superior.

El rol de administrador de la seguridad o el usuario individual pueden agregar el archivo `.mailrc` a `.copy_files` o a `.link_files`. Para obtener una descripción de estos archivos, consulte la página del comando man `updatehome`(1M). Para obtener sugerencias de configuración, consulte "Archivos `.copy_files` y `.link_files`" en la página 84.

- El lector de correo se puede ejecutar en cualquier etiqueta del sistema. Es necesario realizar algunas tareas de configuración para conectar un cliente de correo al servidor.

  Por ejemplo, para utilizar Mozilla para el correo de varios niveles es necesario que configure un cliente de correo de Mozilla en cada etiqueta a fin de especificar el servidor de correo. El servidor de correo puede ser el mismo o uno diferente para cada una de las etiquetas, pero el servidor debe estar especificado.
- La herramienta de listas de correo de Solaris Management Console administra los alias de correo.

  Según el ámbito de la caja de herramientas de Solaris Management Console seleccionada, puede actualizar el archivo local `/etc/aliases` o la entrada de LDAP en el Oracle Directory Server Enterprise Edition.
- El software Trusted Extensions comprueba las etiquetas del host y del usuario antes de enviar o reenviar correo.
  - El software comprueba que el correo se encuentre dentro del rango de acreditación del host. Las comprobaciones se describen en esta lista y en el Capítulo 13, "Gestión de redes en Trusted Extensions (tareas)".
  - El software comprueba que el correo se encuentre entre la autorización de la cuenta y la etiqueta mínima.
  - Los usuarios pueden leer el correo electrónico que se recibe dentro del rango de acreditación. Durante una sesión, los usuarios pueden leer el correo solamente en su etiqueta actual.

    Para ponerse en contacto con un usuario común mediante correo electrónico, un rol administrativo debe enviar un correo desde un espacio de trabajo que se encuentre en una etiqueta que el usuario pueda leer. Por lo general, la etiqueta predeterminada del usuario es una buena opción.

CAPÍTULO 15

Gestión de impresión con etiquetas (tareas)

En este capítulo se describe cómo utilizar el software de Trusted Extensions para configurar la impresión con etiquetas. Además, se explica cómo configurar los trabajos de impresión sin opciones de etiquetas.

Etiquetas, impresoras e impresión

El software de Trusted Extensions usa etiquetas para controlar el acceso a las impresoras. Las etiquetas se usan para controlar el acceso a las impresoras y a la información sobre los trabajos de impresión en cola. El software también etiqueta el resultado de la impresión. Las páginas del cuerpo y las páginas de la carátula y el ubicador obligatorios tienen etiquetas. Además, las páginas de carátula y ubicador pueden incluir instrucciones de tratamiento.

El administrador del sistema se encarga de la administración básica de las impresoras. El rol de administrador de la seguridad se ocupa de la seguridad de las impresoras, que incluye las etiquetas y el tratamiento del la impresión con etiquetas. Los administradores siguen los procedimientos básicos de administración de impresoras de Oracle Solaris y, luego, asignan etiquetas a los servidores de impresión y a las impresoras.

El software de Trusted Extensions admite la impresión de un solo nivel y también de varios niveles. La impresión de varios niveles se implementa únicamente en la zona global. Para utilizar el servidor de impresión de la zona global, las zonas con etiquetas deben tener un nombre de host distinto del de la zona global. Una manera de obtener un nombre de host distinto es asignar una dirección IP a la zona con etiquetas. La dirección sería distinta de la dirección IP de la zona global.

Restricción del acceso a las impresoras y a la información de trabajos de impresión en Trusted Extensions

Los usuarios y los roles de los sistemas en los que está configurado el software de Trusted Extensions crean trabajos de impresión en la etiqueta de su sesión. Los trabajos de impresión se pueden imprimir solamente en impresoras que reconozcan esa etiqueta. La etiqueta debe estar dentro del rango de etiquetas de la impresora.

Los usuarios y los roles pueden ver los trabajos de impresión que tengan la misma etiqueta que la sesión. En la zona global, un rol puede ver los trabajos cuyas etiquetas estén controladas por la etiqueta de la zona.

Las impresoras que se configuran con el software de Trusted Extensions imprimen etiquetas en el resultado de la impresión. Las impresoras administradas con servidores de impresión sin etiquetas no imprimen etiquetas en el resultado de la impresión. Estas impresoras tienen la misma etiqueta que su servidor sin etiquetas. Por ejemplo, se puede asignar una etiqueta arbitraria a un servidor de impresión de Oracle Solaris en la base de datos `tnrhdb` del servicio de nombres LDAP. Así, los usuarios pueden imprimir los trabajos en esa etiqueta arbitraria con la impresora de Oracle Solaris. Como sucede con las impresoras de Trusted Extensions esas impresoras de Oracle Solaris solamente pueden aceptar trabajos de impresión de los usuarios que trabajan en la etiqueta asignada al servidor de impresión.

Resultado de impresión con etiquetas

Trusted Extensions imprime la información de seguridad en las páginas del cuerpo y en las páginas de carátula y de ubicador. La información proviene de los archivos `label_encodings` y `tsol_separator.ps`.

El administrador de la seguridad puede hacer lo siguiente para modificar los valores predeterminados que establecen las etiquetas y agregan instrucciones de tratamiento al resultado de la impresión:

- Localizar o personalizar el texto de las páginas de carátula y de ubicador
- Especificar etiquetas alternativas que se vayan a imprimir en las páginas del cuerpo o en los diversos campos de las páginas de carátula y de ubicador
- Cambiar u omitir cualquiera de los textos o las etiquetas

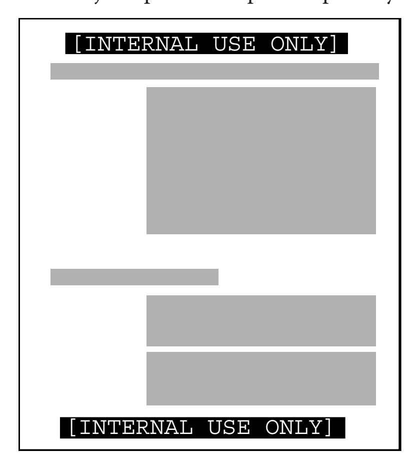
El administrador de la seguridad también puede configurar las cuentas de usuario para que se usen impresoras que no imprimen etiquetas en el resultado. Asimismo, se puede autorizar a los usuarios para que no impriman, de manera selectiva, carátulas o etiquetas en el resultado de la impresión.

Páginas del cuerpo con etiquetas

De manera predeterminada, la clasificación "Protect As" se imprime en la parte superior y en la parte inferior de cada página del cuerpo. La clasificación "Protect As" es la dominante cuando se compara la clasificación de la etiqueta de la tarea con la clasificación `minimum protect as classification`. La clasificación `minimum protect as classification` se define en el archivo `label_encodings`.

Por ejemplo, si el usuario se encuentra en una sesión Internal Use Only , los trabajos de impresión del usuario están en esa etiqueta. Si la clasificación `minimum protect as classification` del archivo `label_encodings` es Public, la etiqueta Internal Use Only se imprime en las páginas del cuerpo.

FIGURA 15–1 Etiqueta del trabajo impresa en la parte superior y en la parte inferior de una página del cuerpo



Páginas de carátula y de ubicador con etiquetas

Las siguientes figuras muestran la página de carátula predeterminada y las variaciones de la página de ubicador predeterminada. Las llamadas identifican las distintas secciones. Tenga en cuenta que la página de ubicador utiliza una línea exterior diferente.

El texto, las etiquetas y las advertencias que aparecen en los trabajos de impresión se pueden configurar. El texto también se puede reemplazar con texto en otro idioma para su localización.

FIGURA 15–2 Página de carátula típica de un trabajo de impresión con etiquetas

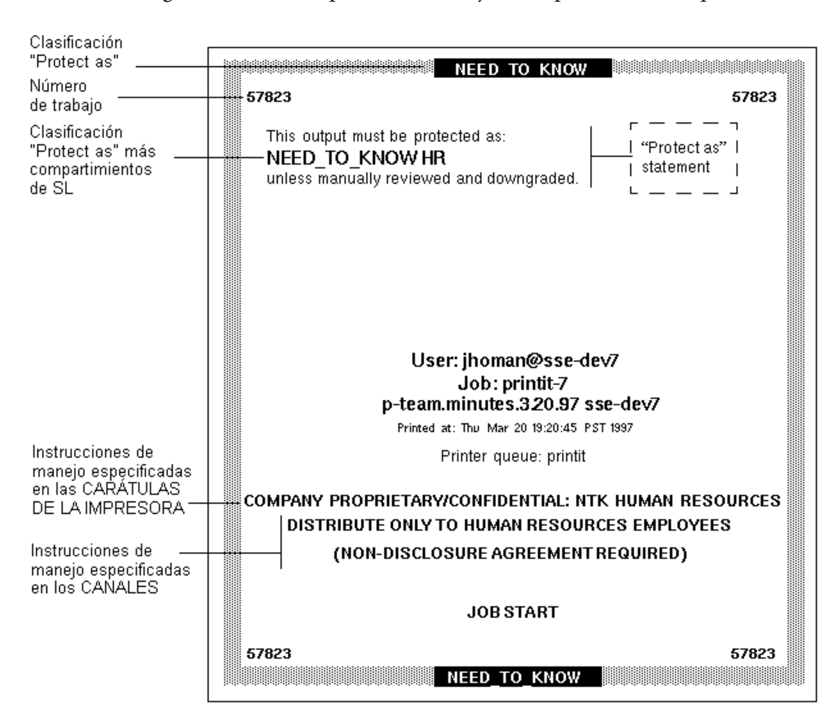
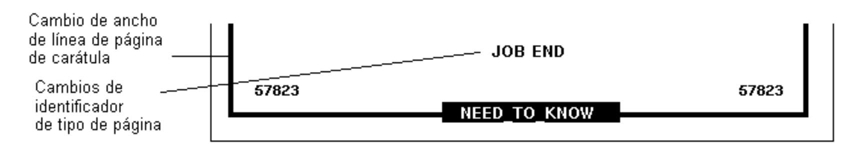


FIGURA 15–3 Diferencias en una página de ubicador



En la siguiente tabla, se muestran los aspectos de la impresión de confianza que el administrador de seguridad puede cambiar mediante la modificación del archivo `/usr/lib/lp/postscript/tsol_separator.ps`.

Nota – Para localizar o internacionalizar el resultado de la impresión, vea los comentarios del archivo `tsol_separator.ps`.

TABLA 15–1 Valores configurables en el archivo `tsol_separator.ps`

Salida	Valor predeterminado	Definición	Para efectuar cambios
`PRINTER BANNERS`	`/Caveats Job_Caveats`	`/Caveats Job_Caveats`	Consulte "Specifying Printer Banners" de *Trusted Extensions Label Administration*.
`CHANNELS`	`/Channels Job_Channels`	`/Channels Job_Channels`	Consulte "Specifying Channels" de *Trusted Extensions Label Administration*.
Etiqueta en la parte superior de las páginas de carátula y de ubicador	`/HeadLabel Job_Protect def`	Consulte la descripción `/PageLabel`.	Igual que para cambiar `/PageLabel`. Consulte también "Specifying the Protect As Classification" de *Trusted Extensions Label Administration*.
Etiqueta en la parte superior de las páginas del cuerpo	`/PageLabel Job_Protect def`	Compara la etiqueta del trabajo con la clasificación `minimum protect as` en el archivo `label_encodings`. Imprime la clasificación más dominante. Contiene compartimientos si la etiqueta del trabajo de impresión tiene compartimientos.	Cambie la definición `/PageLabel` para especificar otro valor. O bien, escriba una cadena que elija. O bien, no imprima nada.

Texto y etiqueta de la instrucción de clasificación "Protect as"	`/Protect Job_Protect def`
	`/Protect_Text1 () def`
	`/Protect_Text2 () def`
		Consulte la descripción `/PageLabel`.
		Texto que aparecerá encima de la etiqueta.
		Texto que aparecerá debajo de la etiqueta.
			Igual que para cambiar `/PageLabel`.
			Reemplace `()` en `Protect_Text1` y `Protect_Text2` con una cadena de texto.

Impresión PostScript de la información de seguridad

La impresión con etiquetas en Trusted Extensions se basa en funciones de impresión de Solaris. En el SO Oracle Solaris, las secuencias de comandos del modelo de la impresora gestionan la creación de la página de la carátula. A fin de implementar las etiquetas, la secuencia de comandos del modelo de la impresora primero convierte el trabajo de impresión en un archivo PostScript. A continuación, el archivo PostScript se manipula para que se inserten etiquetas en las páginas del cuerpo y se creen las páginas de la carátula y del ubicador.

Las secuencias de comandos del modelo de la impresora de Solaris también pueden convertir PostScript al lenguaje original de la impresora. Si la impresora acepta entrada PostScript, el software de Oracle Solaris envía el trabajo a la impresora.+ Si la impresora no acepta entrada PostScript, el software convierte al formato PostScript en una imagen raster. Luego, la imagen raster se convierte al formato de impresora correspondiente.

Dado que el software de PostScript se utiliza para imprimir información de las etiquetas, los usuarios no pueden imprimir archivos PostScript de manera predeterminada. Esta restricción impide que los programadores expertos en PostScript creen un archivo PostScript que modifique las etiquetas en el resultado de la impresión.

El rol de administrador de la seguridad puede invalidar esta restricción mediante la asignación de la autorización `Print Postscript` a cuentas de roles y usuarios de confianza. La autorización se asigna únicamente si se puede confiar en que la cuenta no suplantará las etiquetas en el resultado de la impresión. Además, si a un usuario se le permite imprimir archivos PostScript, debe respetarse la política de seguridad del sitio.

Secuencias de comandos del modelo de la impresora

La secuencia de comandos del modelo de la impresora activa un modelo de impresora específico para proporcionar las páginas de la carátula y del ubicador. Trusted Extensions proporciona cuatro secuencias de comandos:

- `tsol_standard`: para impresoras PostScript conectadas de manera directa; por ejemplo, impresoras conectadas mediante un puerto paralelo
- `tsol_netstandard`: para impresoras PostScript a las que se puede acceder por medio de una red
- `tsol_standard_foomatic`: para impresoras conectadas de manera directa, pero que no imprimen en formato PostScript
- `tsol_netstandard_foomatic`: para impresoras a las que se puede acceder por medio de una red, pero que no imprimen en formato PostScript

Las secuencias de comando `foomatic` se utilizan cuando el nombre del controlador de la impresora comienza con `Foomatic`. Los controladores Foomatic son controladores de impresora PostScript (PPD, PostScript Printer Drivers).

Nota – Cuando agrega una impresora en una zona con etiquetas, “Use PPD” se especifica de manera predeterminada en el gestor de impresión. A continuación se utiliza un PPD para convertir las páginas de la carátula y del ubicador al lenguaje de la impresora.

Filtros de conversión adicionales

Los filtros de conversión convierten los archivos de texto al formato PostScript. Los programas del filtro son programas de confianza que ejecuta el daemon de impresión. Se puede confiar en que las etiquetas y el texto de las páginas de la carátula y del ubicador de los archivos que se convierten a formato PostScript mediante cualquier programa de filtros instalado son auténticos.

El software de Oracle Solaris proporciona la mayoría de los filtros de conversión que el sitio necesita. Igualmente, el rol de administrador del sistema del sitio puede instalar filtros

adicionales. Por lo tanto se puede confiar en que las etiquetas y las páginas de la carátula y del ubicador de estos filtros son auténticas. Para obtener información sobre cómo agregar filtros de conversión, consulte el Capítulo 7, "Customizing LP Printing Services and Printers (Tasks)" de *System Administration Guide: Printing*.

Interoperabilidad de Trusted Extensions con la impresión de Trusted Solaris 8

Los sistemas Trusted Solaris 8 y Trusted Extensions que tienen archivos `label_encodings` compatibles y que se identifican entre sí mediante una plantilla CIPSO pueden usarse recíprocamente para la impresión remota. La siguiente tabla describe cómo configurar los sistemas para activar la impresión. De manera predeterminada, los usuarios no pueden enumerar o cancelar trabajos de impresión en un servidor de impresión remoto del otro sistema operativo. Si desea, puede autorizar a los usuarios para que puedan hacerlo.

Sistema de origen	Sistema de servidor de impresión	Acción	Resultados
Trusted Extensions	Trusted Solaris 8	Configure la impresión: en `tnrhdb` de Trusted Extensions, asigne una plantilla con el rango de etiquetas adecuado al servidor de impresión de Trusted Solaris 8. Puede ser con una etiqueta CIPSO o sin etiquetas.	La impresora de Trusted Solaris 8 puede imprimir trabajos desde un sistema Trusted Extensions dentro del rango de etiquetas de la impresora.
Trusted Extensions	Trusted Solaris 8	Autorice a los usuarios: en el sistema Trusted Extensions, cree un perfil que agregue las autorizaciones necesarias. Asigne el perfil a los usuarios.	Los usuarios de Trusted Extensions pueden enumerar o cancelar los trabajos de impresión que envíen a una impresora de Trusted Solaris 8. Los usuarios no pueden ver ni eliminar trabajos en una etiqueta diferente.
Trusted Solaris 8	Trusted Extensions	Configure la impresión: en `tnrhdb` de Trusted Solaris 8, asigne una plantilla con el rango de etiquetas adecuado al servidor de impresión de Trusted Extensions. Puede ser con una etiqueta CIPSO o sin etiquetas.	La impresora de Trusted Extensions puede imprimir trabajos desde un sistema Trusted Solaris 8 dentro del rango de etiquetas de la impresora.

Sistema de origen	Sistema de servidor de impresión	Acción	Resultados
Trusted Solaris 8	Trusted Extensions	Autorice a los usuarios: en el sistema Trusted Solaris 8, cree un perfil que agregue las autorizaciones necesarias. Asigne el perfil a los usuarios.	Los usuarios de Trusted Solaris 8 pueden enumerar o cancelar los trabajos de impresión que envíen a una impresora de Trusted Extensions. Los usuarios no pueden ver ni eliminar trabajos en una etiqueta diferente.

Interfaces de impresión de Trusted Extensions (referencia)

Los siguientes comandos de usuario se amplían a fin de cumplir con la política de seguridad de Trusted Extensions:

- `cancel`: el emisor de llamada debe ser igual a la etiqueta del trabajo de impresión para cancelar un trabajo. De manera predeterminada, los usuarios comunes pueden cancelar solamente sus propios trabajos.
- `lp`: Trusted Extensions agrega la opción `-o nolabels`. Los usuarios deben estar autorizados para imprimir sin etiquetas. Asimismo, los usuarios deben estar autorizados para usar la opción `-o nobanner`.
- `lpstat`: el emisor de llamada debe ser igual a la etiqueta del trabajo de impresión para obtener el estado de un trabajo. De manera predeterminada, los usuarios comunes pueden ver solamente sus propios trabajos de impresión.

Los siguientes comandos administrativos se amplían a fin de cumplir con la política de seguridad de Trusted Extensions. Al igual que en el SO Oracle Solaris, solamente los roles que incluyen el perfil de derechos de gestión de impresoras pueden ejecutar estos comandos.

- `lpmove`: el emisor de llamada debe ser igual a la etiqueta del trabajo de impresión para mover un trabajo. De manera predeterminada, los usuarios comunes pueden mover solamente sus propios trabajos de impresión.
- `lpadmin`: en la zona global, este comando funciona para todos los trabajos. En una zona etiquetada, el emisor de llamada debe dominar la etiqueta del trabajo de impresión para ver un trabajo y debe ser igual para cambiar un trabajo.

  Trusted Extensions agrega secuencias de comandos del modelo de la impresora a la opción `-m`. Trusted Extensions agrega la opción `-o nolabels`.

- `lpsched`: en la zona global, este comando siempre se ejecuta correctamente. Al igual que en el SO Oracle Solaris, use el comando `svcadm` para activar, desactivar, iniciar o reiniciar el servicio de impresión. En una zona etiquetada, el emisor de llamada debe ser igual a la etiqueta del servicio de impresión para cambiar el servicio de impresión. Para obtener detalles sobre la utilidad de gestión de servicios, consulte las páginas del comando man `smf`(5), `svcadm`(1M) y `svcs`(1).

Trusted Extensions agrega la autorización `solaris.label.print` al perfil de derechos de gestión de impresoras. Se requiere la autorización `solaris.print.unlabeled` para imprimir las páginas del cuerpo sin etiquetas.

Gestión de impresión en Trusted Extensions (mapa de tareas)

Los procedimientos de Trusted Extensions para configurar la impresión se realizan una vez que se completa la configuración de la impresora de Oracle Solaris. El siguiente mapa de tareas hace referencia a las tareas principales que gestionan la impresión con etiquetas.

Tarea	Descripción	Para obtener instrucciones
Configurar impresoras para el resultado con etiquetas.	Activar a los usuarios para que impriman en una impresora de Trusted Extensions. Los trabajos de impresión se marcan con etiquetas.	"Configuración de impresión con etiquetas (mapa de tareas)" en la página 219
Eliminar las etiquetas visibles del resultado de la impresión.	Habilitar a los usuarios para que impriman con una etiqueta específica en una impresora de Oracle Solaris. Los trabajos de impresión no se marcan con etiquetas. O bien, impedir que las etiquetas se impriman en una impresora de Trusted Extensions.	"Reducción de las restricciones de impresión en Trusted Extensions (mapa de tareas)" en la página 233

Configuración de impresión con etiquetas (mapa de tareas)

El siguiente mapa de tareas describe los procedimientos de configuración comunes relativos a la impresión con etiquetas.

Nota – Los clientes de la impresora pueden imprimir solamente los trabajos que se encuentren dentro del rango de etiquetas del servidor de impresión de Trusted Extensions.

Tarea	Descripción	Para obtener instrucciones
Configurar la impresión desde la zona global.	Se crea un servidor de impresión de varios niveles en la zona global.	"Cómo configurar un servidor de impresión de varios niveles y sus impresoras" en la página 220

Tarea	Descripción	Para obtener instrucciones
Configurar la impresión para una red de sistemas.	Crear un servidor de impresión de varios niveles en la zona global y activar zonas con etiquetas para utilizar la impresora.	"Cómo configurar una impresora de red para los clientes Sun Ray" en la página 222
Configurar la impresión para sistemas sin etiquetas en la misma subred que los sistemas con etiquetas.	Activar los sistemas sin etiquetas para que usen la impresora de red.	"Cómo configurar la impresión en cascada en un sistema con etiquetas" en la página 225
Configurar la impresión desde una zona con etiquetas.	Crea un servidor de impresión de una sola etiqueta para una zona con etiquetas.	"Cómo configurar una zona para la impresión con una sola etiqueta" en la página 228
Configurar un cliente de impresión de varios niveles.	Se conecta un host de Trusted Extensions con una impresora.	"Cómo activar un cliente de Trusted Extensions para que acceda a un impresora" en la página 230
Restringir el rango de etiquetas de una impresora.	Se restringe una impresora de Trusted Extensions a un rango de etiquetas menor.	"Cómo configurar un rango de etiquetas restringido para una impresora" en la página 232

▼ Cómo configurar un servidor de impresión de varios niveles y sus impresoras

Las impresoras gestionadas por un servidor de impresión de Trusted Extensions imprimen etiquetas en las páginas del cuerpo, de la carátula y del ubicador. Esta clase de impresoras pueden imprimir los trabajos de impresión dentro del rango de etiquetas del servidor de impresión. Cualquier host de Trusted Extensions que llegue al servidor de impresión puede utilizar las impresoras que están conectadas al servidor.

Antes de empezar Determine el servidor de impresión para su red de Trusted Extensions. Debe estar con el rol de administrador del sistema en la zona global de este servidor de impresión.

1. **Inicie Solaris Management Console.**

   Para obtener detalles, consulte "Cómo administrar el sistema local con Solaris Management Console" en la página 55.

2. **Seleccione la caja de herramientas Files.**

   El título de la caja de herramientas incluye `Scope=Files, Policy=TSOL`.

3 Active la impresión de varios niveles mediante la configuración de la zona global con el puerto del servidor de impresión, 515/tcp.

Cree un puerto de varios niveles (MLP) para el servidor de impresión. Para ello, agregue el puerto a la zona global.

a. Vaya a la herramienta Trusted Network Zones.

b. En Multilevel Ports for Zone's IP Addresses, agregue 515/tcp.

c. Haga clic en Aceptar.

4 Defina las características de cada impresora conectada.

Use la línea de comandos. La interfaz gráfica de usuario del gestor de impresiones no funciona en la zona global.

```
# lpadmin -p printer-name -v /dev/null \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
# accept printer-name
# enable printer-name
```

5 Asigne una secuencia de comandos del modelo de la impresora a cada impresora que esté conectada con el servidor de impresión.

La secuencia de comandos del modelo activa las páginas de la carátula y del ubicador para la impresora especificada.

Para obtener una descripción de las secuencias de comandos, consulte "Secuencias de comandos del modelo de la impresora" en la página 216. Si el nombre del controlador de la impresora comienza con `Foomatic`, especifique una de las secuencias de comandos del modelo foomatic. En una línea, utilice el siguiente comando:

```
$ lpadmin -p printer \
 -m { tsol_standard | tsol_netstandard |
      tsol_standard_foomatic | tsol_netstandard_foomatic }
```

Si el rango de etiquetas predeterminado que va de `ADMIN_LOW` a `ADMIN_HIGH` es aceptable para todas las impresoras, significa que se completó la configuración de las etiquetas.

6 Configure la impresora en cada zona con etiquetas donde se permite la impresión.

Utilice la dirección IP `all-zones` como servidor de impresión para la zona global.

a. Inicie sesión como root en la consola de la zona etiquetada.

```
# zlogin -C labeled-zone
```

b. Agregue la impresora a la zona.

```
# lpadmin -p printer-name -s all-zones-IP-address
```

c. (Opcional) Establezca la impresora como predeterminada.

```
# lpadmin -d printer-name
```

7 En cada zona, pruebe la impresora.

Nota – A partir de la versión Solaris 10 7/10, los archivos que tengan una etiqueta administrativa, ya sea `ADMIN_HIGH` o `ADMIN_LOW`, imprimen `ADMIN_HIGH` en el cuerpo de la copia impresa. Las páginas de la carátula y del ubicador tienen la etiqueta máxima y los compartimientos del archivo `label_encodings`.

Como usuario `root` y como usuario común, realice los siguientes pasos:

a. **Imprima los archivos sin formato de la línea de comandos.**

b. **Imprima los archivos desde las aplicaciones, como Beehive, y desde el explorador y el editor.**

c. **Verifique que las páginas de la carátula y del ubicador, y las carátulas de seguridad se impriman correctamente.**

Véase también

- **Limitar el rango de etiquetas de la impresora**: "Cómo configurar un rango de etiquetas restringido para una impresora" en la página 232
- **Impedir el resultado con etiquetas**: "Reducción de las restricciones de impresión en Trusted Extensions (mapa de tareas)" en la página 233
- **Usar esta zona como servidor de impresión**: "Cómo activar un cliente de Trusted Extensions para que acceda a un impresora" en la página 230

▼ Cómo configurar una impresora de red para los clientes Sun Ray

Este procedimiento configura una impresora PostScript en un servidor Sun Ray que tiene una sola interfaz `all-zones`. La impresora se pone a disposición de todos los usuarios de los clientes Sun Ray de este servidor. La configuración inicial se realiza en la zona global. Una vez que se configura la zona global, se configuran todas las zonas con etiquetas para que utilicen la impresora.

Antes de empezar Debe estar conectado en una sesión de varios niveles en Trusted CDE.

1 En la zona global, asigne una dirección IP a la impresora de red.

Para obtener instrucciones, consulte el Capítulo 5, "Setting Up Printers by Using LP Print Commands (Tasks)" de *System Administration Guide: Printing*.

2 Inicie Solaris Management Console.

- Para obtener instrucciones, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

- Seleccione la caja de herramientas `Scope=Files, Policy=TSOL` e inicie sesión.

3 Asigne la impresora a la plantilla `admin_low`.

a. En la herramienta Computers and Networks, haga doble clic en Security Templates.

b. Haga doble clic en `admin_low`.

c. En la ficha Hosts Assigned to Template, agregue la dirección IP de la impresora.

Para obtener más información, lea la ayuda en pantalla que se encuentra en el panel izquierdo.

4 Agregue el puerto de la impresora a la interfaz compartida de la zona global.

a. En la herramienta Computers and Networks, haga doble clic en Trusted Network Zones.

b. Haga doble clic en `global`.

c. En la lista Multilevel Ports for Shared IP Addresses, agregue el puerto `515`, protocolo `tcp`.

5 Verifique que las asignaciones de Solaris Management Console estén en el núcleo.

```
# tninfo -h printer-IP-address
   IP address= printer-IP-address
   Template = admin_low

# tninfo -m global
   private: 111/tcp;111/udp;513/tcp;515/tcp;631/tcp;2049/tcp;6000-6050/tcp;
7007/tcp;7010/tcp;7014/tcp;7015/tcp;32771/tcp;32776/ip
   shared: 515/tcp;6000-6050/tcp;7007/tcp;7010/tcp;7014/tcp;7015/tcp
```

Nota – Los puertos de varios niveles (MLP) privados y compartidos adicionales, como `6055` y `7007`, cumplen con los requerimientos de Sun Ray.

---

6 Asegúrese de que los servicios de impresión estén activados en la zona global.

```
# svcadm enable print/server
# svcadm enable rfc1179
```

7 Si el sistema se instaló con `netservices limited`, active la impresora para que llegue a la red.

El servicio `rfc1179` debe recibir las direcciones que no sean de `localhost`. El servicio LP recibe solamente una conducción con nombre.

```
# inetadm -m svc:/application/print/rfc1179:default bind_addr=’’
# svcadm refresh rfc1179
```

Nota – Si ejecuta `netservices open`, el comando anterior genera el siguiente error: `Error: "inetd" property group missing`.

---

8 Active a todos los usuarios para que impriman en PostScript.

En Trusted Editor, cree el archivo `/etc/default/print` y agregue la siguiente línea:

```
PRINT_POSTSCRIPT=1
```

Las aplicaciones como Beehive y `gedit` crean una salida de PostScript.

9 Agregue todos los filtros LP al servicio de impresión.

En la zona global, ejecute esta secuencia de comandos C-Shell:

```
csh
    cd /etc/lp/fd/
    foreach a (*.fd)
        lpfilter -f $a:r -F $a
    end
```

10 Agregue una impresora en la zona global.

Use la línea de comandos. La interfaz gráfica de usuario del gestor de impresiones no funciona en la zona global.

```
# lpadmin -p printer-name -v /dev/null -m tsol_netstandard \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
# accept printer-name
# enable printer-name
```

11 (Opcional) Establezca la impresora como predeterminada.

```
# lpadmin -d printer-name
```

12 En cada zona con etiquetas, configure la impresora.

Utilice la dirección IP `all-zones` como servidor de impresión para la zona global. Si su NIC de `all-zones` es una interfaz de red virtual (VNI, Virtual Network Interface), utilice la dirección IP para la VNI como argumento de la opción `-s`.

a. Inicie sesión como root en la consola de la zona etiquetada.

```
# zlogin -C labeled-zonename
```

b. Agregue la impresora a la zona.

```
# lpadmin -p printer-name -s global-zone-shared-IP-address
```

c. (Opcional) Establezca la impresora como predeterminada.

```
# lpadmin -d printer-name
```

13 En cada zona, pruebe la impresora.

Nota – A partir de la versión Solaris 10 7/10, los archivos que tengan una etiqueta administrativa, ya sea `ADMIN_HIGH` o `ADMIN_LOW`, imprimen `ADMIN_HIGH` en el cuerpo de la copia impresa. Las páginas de la carátula y del ubicador tienen la etiqueta máxima y los compartimientos del archivo `label_encodings`.

Como usuario `root` y como usuario común, realice los siguientes pasos:

a. **Imprima los archivos sin formato de la línea de comandos.**

b. **Imprima los archivos desde las aplicaciones, como Beehive, y desde el explorador y el editor.**

c. **Verifique que las páginas de la carátula y del ubicador, y las carátulas de seguridad se impriman correctamente.**

Ejemplo 15–1 Determinación del estado de una impresora de red

En este ejemplo, el administrador verifica el estado de la impresora de red desde la zona global y desde una zona con etiquetas.

```
global # lpstat -t
    scheduler is running
    system default destination: math-printer
    system for _default: trusted1 (as printer math-printer)
    device for math-printer: /dev/null
    character set
    default accepting requests since Feb 28 00:00 2008
    lex accepting requests since Feb 28 00:00 2008
    printer math-printer is idle. enabled since Feb 28 00:00 2008. available.

Solaris1# lpstat -t
   scheduler is not running
   system default destination: math-printer
   system for _default: 192.168.4.17 (as printer math-printer)
   system for math-printer: 192.168.4.17
   default accepting requests since Feb 28 00:00 2008
   math-printer accepting requests since Feb 28 00:00 2008
   printer _default is idle. enabled since Feb 28 00:00 2008. available.
   printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

▼ Cómo configurar la impresión en cascada en un sistema con etiquetas

La impresión en cascada proporciona la capacidad de imprimir desde una sesión de escritorio de Windows a una interfaz de zona con etiquetas de Trusted Extensions, donde la dirección IP de la zona de la interfaz física actúa como administrador de trabajos de impresión. El receptor del puerto de varios niveles (MLP) que se encuentra en la dirección IP de la zona de la interfaz

física se comunica con el subsistema de impresión de Trusted Extensions e imprime el archivo con el encabezado con etiquetas y las hojas del ubicador que corresponden.

Este procedimiento activa los sistemas sin etiquetas que están en la misma subred que los sistemas con etiquetas para que usen la impresora de red con etiquetas. El servicio `rfc1179` administra la impresión en cascada. Debe realizar este procedimiento en todas las zonas con etiquetas desde las que permita la impresión en cascada.

Antes de empezar Debe haber terminado con "Cómo configurar una impresora de red para los clientes Sun Ray" en la página 222.

1 **Inicie sesión como root en la consola de la zona etiquetada.**

```
# zlogin -C labeled-zonename
```

2 **Elimine la dependencia del servicio `rfc1179` en relación con el servicio print/server.**

```
labeled-zone # cat <<EOF | svccfg
      select application/print/rfc1179
      delpg lpsched
      end
   EOF

labeled-zone # svcadm refresh application/print/rfc1179
```

3 **Compruebe que el servicio `rfc1179` esté activado.**

```
labeled-zone # svcadm enable rfc1179
```

4 **Si la zona con etiquetas se instaló con `netservices limited`, active la impresora para que llegue a la red.**

El servicio `rfc1179` debe recibir las direcciones que no sean de `localhost`. El servicio LP recibe solamente una conducción con nombre.

```
# inetadm -m svc:/application/print/rfc1179:default bind_addr=''
# svcadm refresh rfc1179
```

Nota – Si ejecuta `netservices open`, el comando anterior genera el siguiente mensaje: `Error: "inetd" property group missing`.

---

5 **Configure la impresión en cascada desde la zona con etiquetas.**

```
labeled-zone # lpset -n system -a spooling-type=cascade printer-name
```

Este comando actualiza el archivo `/etc/printers.conf` de la zona.

6 **Pruebe un sistema Oracle Solaris que se encuentre en la misma subred que esta zona con etiquetas.**

Por ejemplo, pruebe el sistema `Solaris1`. Este sistema se encuentra en la misma subred que la zona `internal`. Los parámetros de configuración son los siguientes:

- La dirección IP de `math-printer` es 192.168.4.6
- La dirección IP de `Solaris1` es 192.168.4.12
- La dirección IP de la zona `internal` es 192.168.4.17

```
Solaris1# uname -a
SunOS Solaris1 Generic_120011-11 sun4u sparc SUNW,Sun-Blade-1000
Solaris1# lpadmin -p math-printer -s 192.168.4.17
Solaris1# lpadmin -d math-printer

Solaris1# lpstat -t
   scheduler is not running
   system default destination: math-printer
   system for _default: 192.168.4.17 (as printer math-printer)
   system for math-printer: 192.168.4.17
   default accepting requests since Feb 28 00:00 2008
   math-printer accepting requests since Feb 28 00:00 2008
   printer _default is idle. enabled since Feb 28 00:00 2008. available.
   printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

- **Pruebe el comando `lp`.**

  ```
  Solaris1# lp /etc/hosts
     request id is math-printer-1 (1 file)
  ```

- **Pruebe la impresión desde las aplicaciones, como Beehive, y desde el explorador.**

7 **Pruebe un servidor Windows 2003 que se encuentre en la misma subred que esta zona con etiquetas.**

a. **Configure la impresora en el servidor Windows.**

Mediante la interfaz gráfica de usuario, vaya a Inicio->Configuración->Impresoras y faxes.

Especifique la siguiente configuración para la impresora:

- Agregar una impresora
- Impresora local conectada a este equipo
- Crear nuevo puerto: seleccione Puerto TCP/IP estándar
- Nombre de impresora o dirección IP: escriba 192.168.4.17, que es la dirección IP de la zona con etiquetas
- Nombre del puerto: acepte el valor predeterminado
- Se requiere información adicional sobre puertos: acepte el valor predeterminado
  - Tipo de dispositivo = Personalizado
  - Configuración: Protocolo = LPR
  - Configuración LPR: Nombre de cola = math-printer, que es el nombre de cola de UNIX

- Cuenta de bytes LPR activada

Para terminar de completar las indicaciones, especifique el fabricante, el modelo, el controlador y los demás parámetros de la impresora.

8 **Para probar la impresora, selecciónela desde una aplicación.**

Por ejemplo, pruebe el sistema `winserver` que está en la misma subred que la zona `internal`. Los parámetros de configuración son los siguientes:

- La dirección IP de `math-printer` es 192.168.4.6
- La dirección IP de `winserver` es 192.168.4.200
- La dirección IP de la zona `internal` es 192.168.4.17

```
winserver C:/> ipconfig
Windows IP Configuration
   Ethernet adapter TP-NIC:
      Connection-specific DNS Suffix  . :
      IP Address. . . . . . . . . . . . : 192.168.4.200
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      Default Gateway . . . . . . . . . : 192.168.4.17
```

▼ Cómo configurar una zona para la impresión con una sola etiqueta

Antes de empezar La zona no debe compartir una dirección IP con la zona global. Debe estar con el rol de administrador del sistema en la zona global.

1 **Agregue un espacio de trabajo.**

Para obtener detalles, consulte "How to Add a Workspace at a Particular Label" de *Trusted Extensions User's Guide*.

2 **Cambie la etiqueta del espacio de trabajo nuevo por la etiqueta de la zona que será servidor de impresión para esa etiqueta.**

Para obtener detalles, consulte "How to Change the Label of a Workspace" de *Trusted Extensions User's Guide*.

3 **Defina las características de las impresoras conectadas.**

a. **En la etiqueta de la zona, inicie el gestor de impresión.**

De manera predeterminada, la casilla "Use PPD" se encuentra seleccionada. El sistema busca el controlador adecuado para la impresora.

b. (Opcional) A fin de especificar un controlador diferente para una impresora, realice lo siguiente:

i. Anule la selección de "Use PPD".

ii. Defina la marca y el modelo de la impresora que usa un controlador diferente.

En el gestor de impresión, debe proporcionar los valores de los dos primeros campos, y luego el gestor de impresión proporciona el nombre del controlador.

`Printer Make`	*manufacturer*
`Printer Model`	*manufacturer-part-number*
`Printer Driver`	*automatically filled in*

4 Asigne una secuencia de comandos del modelo de la impresora a cada impresora que esté conectada a la zona.

La secuencia de comandos del modelo activa las páginas de la carátula y del ubicador para la impresora especificada.

Para conocer las opciones de secuencias de comandos, consulte "Secuencias de comandos del modelo de la impresora" en la página 216. Si el nombre del controlador de la impresora comienza con `Foomatic`, especifique una de las secuencias de comandos del modelo foomatic. Utilice el siguiente comando:

```
$ lpadmin -p printer -m model
```

Las impresoras conectadas pueden imprimir trabajos únicamente en la etiqueta de la zona.

5 Pruebe la impresora.

Nota – A partir de la versión Solaris 10 7/10, los archivos que tengan una etiqueta administrativa, ya sea `ADMIN_HIGH` o `ADMIN_LOW`, imprimen `ADMIN_HIGH` en el cuerpo de la copia impresa. Las páginas de la carátula y del ubicador tienen la etiqueta máxima y los compartimientos del archivo `label_encodings`.

Como usuario `root` y como usuario común, realice los siguientes pasos:

a. Imprima los archivos sin formato de la línea de comandos.

b. Imprima los archivos desde las aplicaciones, como Beehive, y desde el explorador y el editor.

c. Verifique que las páginas de la carátula y del ubicador, y las carátulas de seguridad se impriman correctamente.

Véase también **Impedir el resultado con etiquetas**: "Reducción de las restricciones de impresión en Trusted Extensions (mapa de tareas)" en la página 233

▼ Cómo activar un cliente de Trusted Extensions para que acceda a un impresora

Inicialmente, únicamente la zona en la que se configuró un servidor de impresión puede imprimir en las impresoras de ese servidor. El administrador del sistema debe agregar explícitamente el acceso a esas impresoras para otras zonas y sistemas. Las posibilidades son las siguientes:

- Para una zona global, agregue el acceso a las impresoras que estén conectadas a una zona global en un sistema diferente.
- Para una zona con etiquetas, agregue el acceso a las impresoras que estén conectadas a la zona global del sistema.
- Para una zona con etiquetas, agregue el acceso a una impresora para la que una zona remota de la misma etiqueta esté configurada.
- Para una zona con etiquetas, agregue el acceso a las impresoras que estén conectadas a una zona global en un sistema diferente.

Antes de empezar Debe haber un servidor de impresión configurado con un rango de etiquetas o una sola etiqueta, y las impresoras conectadas a ese servidor deben estar configuradas. Para obtener detalles, consulte lo siguiente:

- "Cómo configurar un servidor de impresión de varios niveles y sus impresoras" en la página 220
- "Cómo configurar una zona para la impresión con una sola etiqueta" en la página 228
- "Cómo asignar una etiqueta a un servidor de impresión sin etiquetas" en la página 235

Debe estar en el rol de administrador del sistema en la zona global o debe poder asumirlo.

1 Realice los procedimientos necesarios para activar el acceso las impresoras en los sistemas.

- **Configure la zona global en un sistema que no sea servidor de impresión y use la zona global de otro sistema para acceder a las impresoras.**

  a. En el sistema que no tiene acceso a las impresoras, asuma el rol de administrador del sistema.

  b. Agregue el acceso a la impresora que está conectada al servidor de impresión de Trusted Extensions.

  ```
  $ lpadmin -s printer
  ```

- **Configure una zona con etiquetas a fin de usar su zona global para acceder a una impresora.**

  a. **Cambie la etiqueta del espacio de trabajo de rol por la etiqueta de la zona con etiquetas.**

     Para obtener detalles, consulte "How to Change the Label of a Workspace" de *Trusted Extensions User's Guide*.

  b. **Agregue el acceso a la impresora.**

     ```
     $ lpadmin -s printer
     ```

- **Configure una zona con etiquetas a fin de usar la zona con etiquetas de otro sistema para acceder a una impresora.**

  Las etiquetas de las zonas deben ser idénticas.

  a. **En el sistema que no tiene acceso a las impresoras, asuma el rol de administrador del sistema.**

  b. **Cambie la etiqueta del espacio de trabajo de rol por la etiqueta de la zona con etiquetas.**

     Para obtener detalles, consulte "How to Change the Label of a Workspace" de *Trusted Extensions User's Guide*.

  c. **Agregue el acceso a la impresora que está conectada al servidor de impresión de la zona con etiquetas remota.**

     ```
     $ lpadmin -s printer
     ```

- **Configure una zona con etiquetas a fin de usar un servidor de impresión sin etiquetas para acceder a una impresora.**

  La etiqueta de la zona debe ser idéntica a la etiqueta del servidor de impresión.

  a. **En el sistema que no tiene acceso a las impresoras, asuma el rol de administrador del sistema.**

  b. **Cambie la etiqueta del espacio de trabajo de rol por la etiqueta de la zona con etiquetas.**

     Para obtener detalles, consulte "How to Change the Label of a Workspace" de *Trusted Extensions User's Guide*.

  c. **Agregue el acceso a la impresora que está conectada al servidor de impresión con etiquetas asignadas de manera arbitraria.**

     ```
     $ lpadmin -s printer
     ```

2 Pruebe las impresoras.

A partir de la versión Solaris 10 7/10, los archivos que tengan una etiqueta administrativa, ya sea `ADMIN_HIGH` o `ADMIN_LOW`, imprimen `ADMIN_HIGH` en el cuerpo de la copia impresa. Las páginas de la carátula y del ubicador tienen la etiqueta máxima y los compartimientos del archivo `label_encodings`.

En cada cliente, pruebe que la impresión funcione para los usuarios `root` y los roles en la zona global, y para los usuarios `root`, los roles y los usuarios comunes en las zonas con etiquetas.

a. **Imprima los archivos sin formato de la línea de comandos.**

b. **Imprima los archivos desde las aplicaciones, como Beehive, y desde el explorador y el editor.**

c. **Verifique que las páginas de la carátula y del ubicador, y las carátulas de seguridad se impriman correctamente.**

▼ Cómo configurar un rango de etiquetas restringido para una impresora

El rango de etiquetas predeterminado de la impresora es de `ADMIN_LOW` a `ADMIN_HIGH`. Este procedimiento reduce el rango de etiquetas de las impresoras controladas mediante un servidor de impresión de Trusted Extensions.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 Inicie Device Allocation Manager.

- **Seleccione la opción Allocate Device en el menú Trusted Path.**
- **En Trusted CDE, inicie la acción Device Allocation Manager del subpanel Tools en el panel frontal.**

2 Haga clic en el botón Device Administration para ver el cuadro de diálogo Device Allocation: Administration.

3 Escriba un nombre para la impresora nueva.

Si la impresora no está conectada al sistema, busque el nombre de la impresora.

4 Haga clic en el botón Configure para ver el cuadro de diálogo Device Allocation: Configuration.

5 Cambie el rango de etiquetas de la impresora.

a. Haga clic en el botón Min Label para cambiar la etiqueta mínima.

Seleccione una etiqueta del generador de etiquetas. Para obtener información sobre el generador de etiquetas, consulte "Generador de etiquetas en Trusted Extensions" en la página 43.

b. Haga clic en el botón Max Label para cambiar la etiqueta máxima.

6 Guarde los cambios.

a. Haga clic en OK en el cuadro de diálogo Configuration.

b. Haga clic en OK en el cuadro de diálogo Administration.

7 Cierre Device Allocation Manager.

Reducción de las restricciones de impresión en Trusted Extensions (mapa de tareas)

Las siguientes tareas son opcionales. Disminuyen la seguridad de la impresión que Trusted Extensions proporciona de manera predeterminada cuando se instala el software.

Tarea	Descripción	Para obtener instrucciones
Configurar una impresora para que no etiquete el resultado.	Impedir la impresión de información de seguridad en las páginas del cuerpo y eliminar las páginas de la carátula y del ubicador.	"Cómo eliminar las etiquetas del resultado de la impresión" en la página 234
Configurar las impresoras en una sola etiqueta sin resultado con etiquetas.	Habilitar a los usuarios para que impriman con una etiqueta específica en una impresora de Oracle Solaris. Los trabajos de impresión no se marcan con etiquetas.	"Cómo asignar una etiqueta a un servidor de impresión sin etiquetas" en la página 235
Eliminar las etiquetas visibles de las páginas del cuerpo.	Modificar el archivo `tsol_separator.ps` para impedir que las páginas del cuerpo de todos los trabajos de impresión que se envían desde un host de Trusted Extensions tengan etiquetas.	"Cómo eliminar las etiquetas de las páginas de todos los trabajos de impresión" en la página 236
Suprimir las páginas de la carátula y del ubicador.	Autorizar a usuarios específicos para que impriman trabajos sin las páginas de la carátula y del ubicador.	"Cómo suprimir las páginas de la carátula y del ubicador para usuarios específicos" en la página 237

Tarea	Descripción	Para obtener instrucciones
Activar usuarios de confianza para que impriman trabajos sin etiquetas.	Autorizar a usuarios específicos o a todos los usuarios de un sistema en particular para que impriman trabajos sin etiquetas.	"Cómo activar a usuarios específicos para que supriman las etiquetas de las páginas" en la página 236
Activar la impresión de archivos PostScript.	Autorizar a usuarios específicos o a todos los usuarios de un sistema en particular para que impriman archivos PostScript.	"Cómo activar a los usuarios para que impriman archivos PostScript en Trusted Extensions" en la página 237
Asignar autorizaciones de impresión.	Activar a los usuarios para que omitan las restricciones de impresión predeterminadas.	"Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 96 "Cómo modificar los valores predeterminados de `policy.conf`" en la página 89

▼ Cómo eliminar las etiquetas del resultado de la impresión

Las impresoras que no tienen una secuencia de comandos del modelo de la impresora de Trusted Extensions no imprimen las páginas de la carátula y del ubicador con etiquetas. Tampoco se incluyen etiquetas en las páginas del cuerpo.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

- **En la etiqueta adecuada, realice una de las siguientes acciones:**
  - **Desde el servidor de impresión, detenga la impresión de la carátula por completo.**

    ```
    $ lpadmin -p printer -o nobanner=never
    ```

    Las páginas del cuerpo se siguen etiquetando.

  - **Establezca la secuencia de comandos del modelo de la impresora en una secuencia de comandos de Oracle Solaris.**

    ```
    $ lpadmin -p printer  \
    -m { standard | netstandard | standard_foomatic | netstandard_foomatic }
    ```

    No aparecen etiquetas en el resultado de la impresión.

▼ Cómo asignar una etiqueta a un servidor de impresión sin etiquetas

El servidor de impresión de Oracle Solaris es un servidor de impresión sin etiquetas al cual se le puede asignar una etiqueta para que Trusted Extensions acceda a la impresora en esa etiqueta. Las impresoras conectadas a un servidor de impresión sin etiquetas pueden imprimir trabajos solamente en la etiqueta que esté asignada al servidor de impresión. Los trabajos se imprimen sin las etiquetas ni las páginas del ubicador, y puede que se impriman sin las páginas de la carátula. Si un trabajo se imprime con la página de la carátula, es porque la página no contiene ninguna información de seguridad.

El sistema Trusted Extensions puede configurarse para que envíen trabajos a una impresora gestionada con un servidor de impresión sin etiquetas. Los usuarios pueden imprimir los trabajos en la impresora sin etiquetas en la etiqueta que el administrador de la seguridad asigna al servidor de impresión.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Abra la consola Solaris Management Console en el ámbito adecuado.**

   Para obtener detalles, consulte "Initialize the Solaris Management Console Server in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

2. **En System Configuration, diríjase hasta la herramienta Computers and Networks.**

   Escriba una contraseña cuando se le solicite.

3. **Asigne una plantilla sin etiquetas en el servidor de impresión.**

   Para obtener detalles, consulte "Cómo asignar una plantilla de seguridad a un host o a un grupo de hosts" en la página 190.

   Elija una etiqueta. Los usuarios que trabajen en ese etiqueta podrán enviar los trabajos de impresión a la impresora de Oracle Solaris en la etiqueta del servidor de impresión. Las páginas no se imprimen con etiquetas, y las páginas de la carátula y del ubicador tampoco forman parte del trabajo de impresión.

Ejemplo 15–2 Envío de trabajos de impresión públicos a una impresora sin etiquetas

Los archivos que se encuentran disponibles para el público en general se pueden imprimir en una impresora sin etiquetas. En este ejemplo, los responsables de marketing de una organización necesitan producir documentos que no tengan etiquetas impresas en la parte superior y en la parte inferior de las páginas.

El administrador de la seguridad asigna una plantilla con el tipo de host sin etiquetas al servidor de impresión Oracle Solaris. La plantilla se describe en el Ejemplo 13–6. La etiqueta arbitraria de la plantilla es `PUBLIC`. La impresora `pr-nolabel1` está conectada a este servidor de

impresión. Los trabajos de impresión de los usuarios de la zona `PUBLIC` se imprimen en la impresora `pr-nolabel1` sin etiquetas. Según la configuración de la impresora, los trabajos pueden tener las páginas de la carátula o no tenerlas. Las páginas de la carátula no contienen información de seguridad.

▼ Cómo eliminar las etiquetas de las páginas de todos los trabajos de impresión

Este procedimiento impide que todos los trabajos de impresión de una impresora de Trusted Extensions incluyan etiquetas visibles en las páginas del cuerpo del trabajo de impresión.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 **Edite el archivo `/usr/lib/lp/postscript/tsol_separator.ps`.**

Utilice el editor de confianza. Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

2 **Encuentre la definición de `/PageLabel`.**

Encuentre las siguientes líneas:

```
%% To eliminate page labels completely, change this line to
%% set the page label to an empty string: /PageLabel () def
/PageLabel Job_PageLabel def
```

Nota – El valor `Job_PageLabel` podría ser diferente en el sitio.

---

3 **Reemplace el valor de `/PageLabel` por un paréntesis vacío.**

```
/PageLabel () def
```

▼ Cómo activar a usuarios específicos para que supriman las etiquetas de las páginas

Mediante este procedimiento se activa a un rol o usuario autorizado a imprimir trabajos en una impresora Trusted Extensions sin etiquetas en la parte superior ni en la parte inferior de cada página del cuerpo. Las etiquetas de las páginas se suprimen para todas las etiquetas en las que el usuario puede trabajar.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 **Determine quién tiene permiso para imprimir los trabajos sin las etiquetas de las páginas.**

2 **Autorice a esos roles y usuarios para imprimir los trabajos sin las etiquetas de las páginas.**

Asigne un perfil de derechos que incluya la autorización Print without Label para esos roles y usuarios. Para obtener detalles, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 96.

3 **Indique al rol o al usuario que use el comando `lp` para ejecutar los trabajos de impresión:**

```
% lp -o nolabels staff.mtg.notes
```

▼ Cómo suprimir las páginas de la carátula y del ubicador para usuarios específicos

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 **Cree un perfil de derechos que incluya la autorización Print without Banner.**

Asigne el perfil a cada rol o usuario que tenga permiso para imprimir sin las páginas de la carátula o del ubicador.

Para obtener detalles, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 96.

2 **Indique al rol o al usuario que use el comando `lp` para ejecutar los trabajos de impresión:**

```
% lp -o nobanner staff.mtg.notes
```

▼ Cómo activar a los usuarios para que impriman archivos PostScript en Trusted Extensions

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

● **Utilice uno de los tres métodos siguientes para activar a los usuarios para que impriman archivos PostScript:**

- **Para activar la impresión PostScript en el sistema, modifique el archivo `/etc/default/print`.**

  a. **Cree o modifique el archivo `/etc/default/print`.**

  Utilice el editor de confianza. Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

  b. **Escriba la entrada siguiente:**

  ```
  PRINT_POSTSCRIPT=1
  ```

c. **Guarde el archivo y cierre el editor.**

- **Para autorizar a todos los usuarios a que impriman archivos PostScript desde el sistema, modifique el archivo `/etc/security/policy.conf`.**

  a. **Modifique el archivo `policy.conf`.**

  Utilice el editor de confianza. Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

  b. **Agregue la autorización `solaris.print.ps`.**

  AUTHS_GRANTED=*other-authorizations*,solaris.print.ps

  c. **Guarde el archivo y cierre el editor.**

- **Para activar a un rol o un usuario para que impriman archivos PostScript desde cualquier sistema, proporcione la autorización adecuada solamente al rol o al usuario determinado.**

  Asigne un perfil que incluya la autorización `Print Postscript` al rol o al usuario determinado. Para obtener detalles, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 96.

Ejemplo 15–3 Activación de la impresión PostScript desde un sistema público

En el siguiente ejemplo, el administrador de la seguridad restringió un quiosco público para operar en la etiqueta `PUBLIC`. El sistema también tiene algunos iconos que abren temas de interés. Estos temas se pueden imprimir.

El administrador de la seguridad crea un archivo `/etc/default/print` en el sistema. El archivo tiene una entrada para activar la impresión de archivos PostScript. Ningún usuario necesita una autorización `Print Postscript`.

```
# vi /etc/default/print

# PRINT_POSTSCRIPT=0
PRINT_POSTSCRIPT=1
```



CAPÍTULO 16

Dispositivos en Trusted Extensions (descripción general)

En este capítulo, se describen las extensiones que Trusted Extensions proporciona para la protección de dispositivos.

Protección de los dispositivos con el software Trusted Extensions

En un sistema Oracle Solaris, los dispositivos se pueden proteger mediante la asignación y la autorización. De manera predeterminada, los dispositivos se encuentran disponibles para los usuarios comunes sin necesidad de autorización. Un sistema configurado con la función Trusted Extensions utiliza los mecanismos de protección de dispositivos del SO Oracle Solaris.

Sin embargo, de manera predeterminada, Trusted Extensions requiere que los dispositivos se asignen y que el usuario esté autorizado para usarlos. Además, los dispositivos se protegen mediante etiquetas. Trusted Extensions proporciona una interfaz gráfica de usuario (GUI, Graphical User Interface) para que los administradores puedan gestionar los dispositivos. Es la misma interfaz que utilizan los usuarios para asignar los dispositivos.

Nota – En Trusted Extensions, los usuarios no pueden utilizar los comandos `allocate` y `deallocate`. Los usuarios deben utilizar Device Allocation Manager. En Solaris Trusted Extensions (JDS), el nombre de la interfaz gráfica de usuario es Device Manager.

Para obtener información sobre la protección de dispositivos en Oracle Solaris, consulte el Capítulo 4, "Controlling Access to Devices (Tasks)" de *System Administration Guide: Security Services*.

En el sistema configurado con Trusted Extensions, dos roles protegen los dispositivos.

- El rol de administrador del sistema controla el acceso a los dispositivos periféricos.

  El administrador del sistema permite que los dispositivos sean asignables. Nadie puede usar los dispositivos establecidos como no asignables por el administrador del sistema. Solamente los usuarios autorizados pueden asignar los dispositivos asignables.
- El rol de administrador de la seguridad restringe las etiquetas en las que se puede acceder a un dispositivo y establece la política de dispositivos. El administrador de la seguridad decide quién está autorizado a asignar un dispositivo.

Las siguientes son las principales funciones del control de los dispositivos con el software Trusted Extensions:

- De manera predeterminada, en el sistema Trusted Extensions, un usuario sin autorización no puede asignar dispositivos como unidades de cinta, unidades de CD-ROM o disquetes.

  Un usuario común que cuente con la autorización Allocate Device puede importar o exportar la información de la etiqueta en la que el usuario asigna el dispositivo.
- Los usuarios invocan Device Allocation Manager cuando inician sesión directamente. Para asignar un dispositivo de manera remota, los usuarios deben tener acceso a la zona global. En general, solamente los roles tienen acceso a la zona global.
- Puede que el rango de etiquetas de cada dispositivo esté restringido por el administrador de la seguridad. Los usuarios comunes están limitados a acceder a los dispositivos cuyo rango de etiquetas incluya las etiquetas en las que a los usuarios se les permite trabajar. El rango de etiquetas predeterminado de un dispositivo es de `ADMIN_LOW` a `ADMIN_HIGH`.
- Los rangos de etiquetas se pueden restringir tanto para los dispositivos que son asignables como para los que no son asignables. Entre los dispositivos que no son asignables se encuentran los búferes de trama y las impresoras.

Rangos de etiquetas de dispositivos

Para evitar que los usuarios copien información confidencial, cada dispositivo asignable tiene un rango de etiquetas. Para utilizar un dispositivo asignable, el usuario debe encontrarse operando en una etiqueta que esté dentro del rango de etiquetas del dispositivo. Si no fuera así, se deniega la asignación. La etiqueta actual del usuario se aplica a los datos que se importan o exportan mientras se asigna el dispositivo al usuario. La etiqueta de los datos exportados se muestra cuando el dispositivo se desasigna. El usuario debe colocar una etiqueta en el medio que contiene los datos exportados de manera física.

Efectos del rango de etiquetas en un dispositivo

Para restringir el acceso de inicio de sesión directo por medio de la consola, el administrador de la seguridad puede establecer un rango de etiquetas restringido en el búfer de trama.

Por ejemplo, se puede especificar un rango de etiquetas restringido a fin de limitar el acceso a un sistema de acceso público. El rango de etiquetas permite a los usuarios acceder al sistema solamente en una etiqueta que esté dentro del rango de etiquetas del búfer de trama.

Cuando un host tiene una impresora local, un rango de etiquetas restringido en la impresora limita los trabajos que se pueden imprimir con esa impresora.

Políticas de acceso a dispositivos

Trusted Extensions sigue las mismas políticas de dispositivos que Oracle Solaris. El administrador de la seguridad puede cambiar las políticas predeterminadas y definir políticas nuevas. El comando `getdevpolicy` recupera la información sobre la política de dispositivos y el comando `update_drv` cambia la política de dispositivos. Para obtener más información, consulte "Configuring Device Policy (Task Map)" de *System Administration Guide: Security Services*. Consulte también las páginas del comando man `getdevpolicy`(1M) y `update_drv`(1M).

Secuencias de comandos device-clean

La secuencia de comandos device-clean se ejecuta cuando se asigna o desasigna un dispositivo. Oracle Solaris proporciona secuencias de comandos para unidades de cinta, de CD-ROM y de disquete. Si su sitio agrega tipos de dispositivos asignables al sistema, puede que los dispositivos agregados requieran secuencias de comandos. Para ver las secuencias de comandos existentes, vaya al directorio `/etc/security/lib`. Para obtener más información, consulte "Device-Clean Scripts" de *System Administration Guide: Security Services*.

Para el software Trusted Extensions, las secuencias de comandos device-clean deben cumplir ciertos requisitos. Estos requisitos se describen en la página del comando man `device_clean`(5).

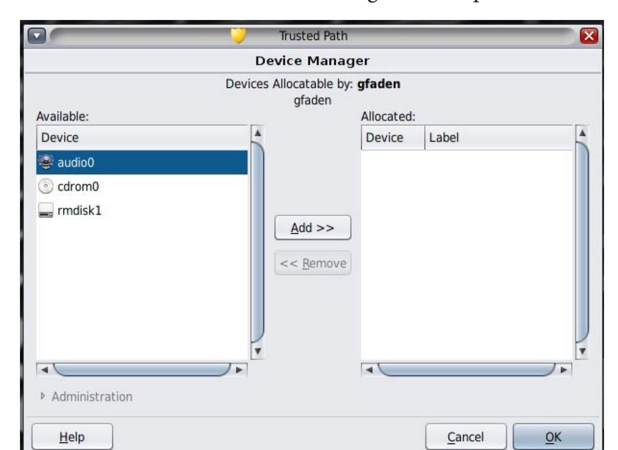
Interfaz gráfica de usuario de Device Allocation Manager

Los administradores usan Device Allocation Manager para administrar dispositivos asignables y no asignables. Asimismo, los usuarios comunes utilizan Device Allocation Manager para asignar y desasignar dispositivos. Los usuarios deben tener la autorización Allocate Device. En el espacio de trabajo de Solaris Trusted Extensions (CDE) , Device Allocation Manager se abre desde el panel frontal. El icono aparece de la siguiente manera:

Asignación de dispositivos

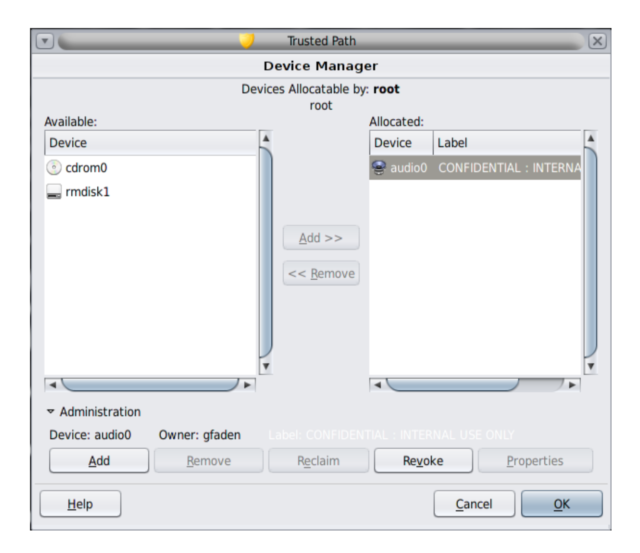
En el espacio de trabajo de Solaris Trusted Extensions (JDS), la interfaz gráfica de usuario se denomina Device Manager. Para iniciar esta interfaz gráfica de usuario, se debe seleccionar Allocate Device en el menú Trusted Path. En Trusted CDE, también puede iniciar la interfaz gráfica de usuario desde el menú Trusted Path. La siguiente figura muestra Device Allocation Manager abierto por un usuario que puede asignar el dispositivo `audio`.

FIGURA 16–1 Device Allocation Manager abierto por un usuario



Los usuarios ven una lista vacía si no están autorizados a asignar dispositivos. Igualmente, una lista vacía podría indicar que los dispositivos asignables se encuentran asignados por otro usuario o están en estado de error. Si un usuario no puede ver un dispositivo en la lista de dispositivos disponibles, debe ponerse en contacto con el administrador responsable.

La función Device Administration está disponible para los roles que tienen una o las dos autorizaciones necesarias para administrar dispositivos. Las autorizaciones de administración son Configure Device Attributes y Revoke or Reclaim Device. La siguiente figura muestra el cuadro de diálogo Device Allocation Administration.



En Solaris Trusted Extensions (JDS), el botón Device Administration se denomina Administration.

Aplicación de la seguridad de los dispositivos en Trusted Extensions

El administrador de la seguridad decide quién puede asignar dispositivos y se asegura de que todos los usuarios autorizados para usar dispositivos reciban la formación necesaria. El usuario es de confianza para realizar lo siguiente:

- Etiquetar y manejar correctamente cualquier medio que contenga información confidencial exportada de modo que la información no esté disponible para ninguna persona que no deba verla.

  Por ejemplo, si la información que tiene la etiqueta `NEED TO KNOW ENGINEERING` se almacena en un disquete, la persona que exporta la información debe colocar en el disco una etiqueta `NEED TO KNOW ENGINEERING` de manera física. El disquete debe almacenarse en un lugar al que puedan acceder únicamente los miembros del grupo de ingeniería que deban saber acerca de la información.

- Asegurarse de que las etiquetas se mantengan de manera apropiada en cualquier información que se importe (lea) desde medios en estos dispositivos.

  Un usuario autorizado debe asignar el dispositivo en la etiqueta que coincida con la etiqueta de la información que se está importando. Por ejemplo, si un usuario asigna una unidad de disquete como `PUBLIC`, el usuario debe importar solamente la información que tenga la etiqueta `PUBLIC`.

El administrador de la seguridad también es responsable de hacer que estos requisitos de seguridad se cumplan como corresponda.

Dispositivos en Trusted Extensions (referencia)

La protección de dispositivos de Trusted Extensions utiliza las interfaces de Oracle Solaris y Trusted Extensions.

Para conocer las interfaces de la línea de comandos de Oracle Solaris, consulte “Device Protection (Reference)” de *System Administration Guide: Security Services*.

Los administradores que no tienen acceso a Device Allocation Manager pueden administrar los dispositivos asignables mediante la línea de comandos. Los comandos `allocate` y `deallocate` tienen opciones administrativas. Para obtener ejemplos, consulte “Forcibly Allocating a Device” de *System Administration Guide: Security Services* y “Forcibly Deallocating a Device” de *System Administration Guide: Security Services*.

Para conocer las interfaces de la línea de comandos de Trusted Extensions, consulte las páginas del comando man `add_allocatable(1M)` y `remove_allocatable(1M)`.

◆ ◆ ◆ CAPÍTULO 17

Gestión de dispositivos para Trusted Extensions (tareas)

En este capítulo se describe cómo administrar y utilizar dispositivos en un sistema configurado con Trusted Extensions.

Control de dispositivos en Trusted Extensions (mapa de tareas)

El siguiente mapa de tareas incluye enlaces a mapas de tareas para administradores y usuarios para el control de dispositivos periféricos.

Tarea	Descripción	Para obtener instrucciones
Usar dispositivos.	Permite usar un dispositivo como rol o como usuario común.	"Uso de dispositivos en Trusted Extensions (mapa de tareas)" en la página 246
Administrar dispositivos.	Permite configurar dispositivos para los usuarios comunes.	"Gestión de dispositivos en Trusted Extensions (mapa de tareas)" en la página 246
Personalizar autorizaciones para dispositivos.	El rol de administrador de la seguridad crea autorizaciones nuevas, las agrega al dispositivo, las ubica en un perfil de derechos y, luego, asigna ese perfil al usuario.	"Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 257

Uso de dispositivos en Trusted Extensions (mapa de tareas)

En Trusted Extensions, todos los roles están autorizados a asignar dispositivos. Como los usuarios, los roles deben usar Device Allocation Manager. El comando `allocate` de Oracle Solaris no funciona en Trusted Extensions. El siguiente mapa de tareas contiene enlaces a procedimientos de usuario para el uso de dispositivos en Trusted Extensions.

Tarea	Para obtener instrucciones
Asignar y desasignar un dispositivo.	"How to Allocate a Device in Trusted Extensions" de *Trusted Extensions User's Guide* "Workspace Switch Area" de *Trusted Extensions User's Guide*
Utilizar medios portátiles para transferir archivos.	"How to Copy Files From Portable Media in Trusted Extensions" de *Trusted Extensions Configuration Guide* "How to Copy Files to Portable Media in Trusted Extensions" de *Trusted Extensions Configuration Guide*

Gestión de dispositivos en Trusted Extensions (mapa de tareas)

El siguiente mapa de tareas describe los procedimientos que se deben llevar a cabo para proteger los dispositivos en el sitio.

Tarea	Descripción	Para obtener instrucciones
Establecer o modificar la política de dispositivos.	Se modifican los privilegios necesarios para acceder a un dispositivo.	"Configuring Device Policy (Task Map)" de *System Administration Guide: Security Services*
Autorizar a los usuarios a asignar un dispositivo.	El rol de administrador de la seguridad asigna un perfil de derechos al usuario con la autorización Allocate Device.	"How to Authorize Users to Allocate a Device" de *System Administration Guide: Security Services*
	El rol de administrador de la seguridad asigna un perfil al usuario con las autorizaciones específicas del sitio.	"Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 257
Configurar un dispositivo.	Se seleccionan funciones de seguridad para proteger el dispositivo.	"Cómo configurar un dispositivo en Trusted Extensions" en la página 247

Tarea	Descripción	Para obtener instrucciones
Revocar o reclamar un dispositivo.	Usar Device Allocation Manager para hacer que un dispositivo esté disponible para su uso.	"Cómo revocar o reclamar un dispositivo en Trusted Extensions" en la página 251
	Se utilizan los comandos de Oracle Solaris para hacer que un dispositivo esté disponible o no para su uso.	"Forcibly Allocating a Device" de *System Administration Guide: Security Services* "Forcibly Deallocating a Device" de *System Administration Guide: Security Services*
Impedir el acceso a un dispositivo asignable.	Se proporciona control de acceso específico a un dispositivo.	Ejemplo 17–4
	Se rechaza el acceso de cualquier usuario a un dispositivo asignable.	Ejemplo 17–1
Proteger las impresoras y los búferes de trama.	Se garantiza que los dispositivos no asignables no se puedan asignar.	"Cómo proteger los dispositivos no asignables en Trusted Extensions" en la página 252
Configurar dispositivos de inicio de sesión de serie.	Activar el inicio de sesiones mediante un puerto de serie.	"Cómo configurar una línea de serie para el inicio de sesiones" en la página 253
Activar un programa reproductor de CD para su uso.	Activar un programa reproductor de audio para que se abra automáticamente al insertar un CD de música.	"Cómo configurar un programa reproductor de audio para que se use en Trusted CDE" en la página 254
Impedir la visualización de File Manager.	Impedir la visualización de File Manager después de la asignación de un dispositivo.	"Cómo impedir la visualización de File Manager después de la asignación de un dispositivo" en la página 255
Utilizar una secuencia de comandos device-clean nueva.	Se agrega una secuencia de comandos nueva en los lugares adecuados.	"Cómo agregar una secuencia de comandos device_clean en Trusted Extensions" en la página 256

▼ Cómo configurar un dispositivo en Trusted Extensions

De manera predeterminada, los dispositivos asignables tienen un rango de etiquetas de `ADMIN_LOW` a `ADMIN_HIGH` y se deben asignar para su uso. Además, los usuarios deben estar autorizados para asignar dispositivos. Estos valores predeterminados se pueden cambiar.

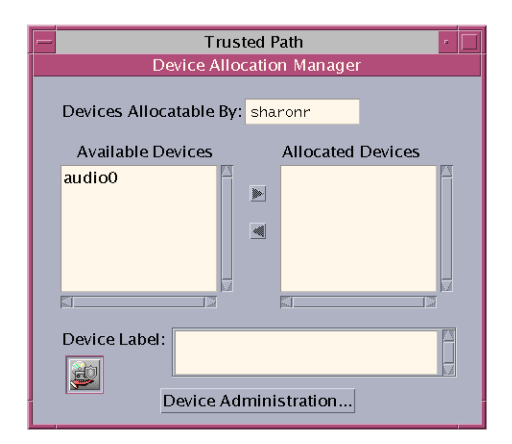
Los siguientes dispositivos se pueden asignar para su uso:

- `audio`*n*: indica un micrófono y un altavoz
- `cdrom`*n*: indica una unidad de CD-ROM
- `floppy`*n*: indica una unidad de disquete
- `mag_tape`*n*: indica una unidad de cinta (transmisión por secuencias)
- `rmdisk`*n*: indica un disco extraíble, como una unidad Jaz o Zip, o medios USB conectables

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

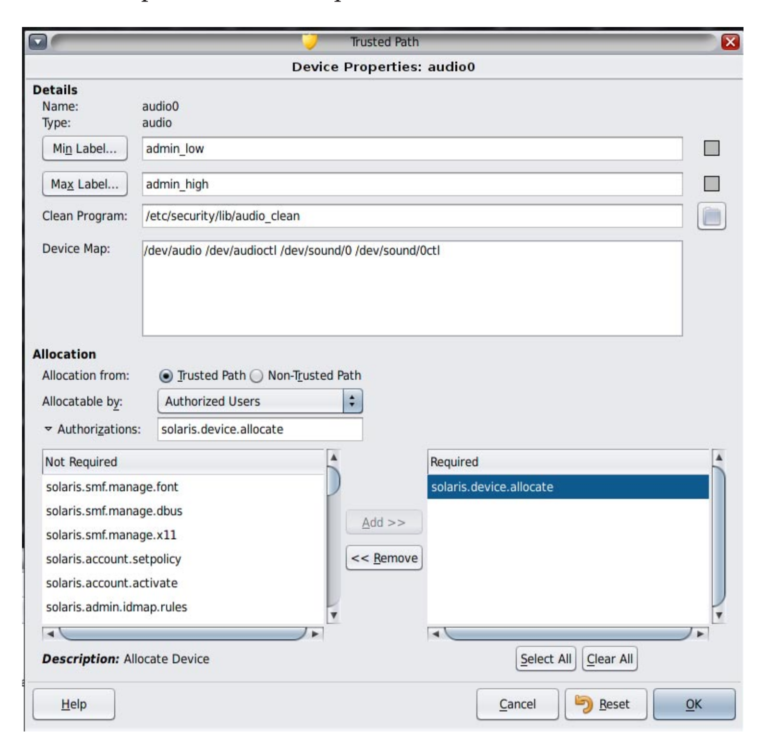
1 En el menú Trusted Path, seleccione Allocate Device.

Aparece Device Allocation Manager.



2 Vea las configuraciones de seguridad predeterminadas.

Haga clic en Device Administration y, a continuación, resalte el dispositivo. La siguiente figura muestra un dispositivo de audio que el rol de usuario `root` está visualizando.



3 (Opcional) Restrinja el rango de etiquetas en el dispositivo.

a. Establezca la etiqueta mínima.

Haga clic en el botón Min Label... y seleccione una etiqueta mínima del generador de etiquetas. Para obtener información sobre el generador de etiquetas, consulte "Generador de etiquetas en Trusted Extensions" en la página 43.

b. Establezca la etiqueta máxima.

Haga clic en el botón Max Label... y seleccione una etiqueta máxima del generador de etiquetas.

4 Especifique si el dispositivo se puede asignar localmente.

En el cuadro de diálogo Device Allocation Configuration, en For Allocations From Trusted Path, seleccione una opción de la lista Allocatable By. De manera predeterminada, la opción Authorized Users está activada. Por lo tanto, el dispositivo es asignable y los usuarios deben estar autorizados.

- **Para hacer que el dispositivo no sea asignable, haga clic en No Users.**

  Si configura una impresora, un búfer de trama u otro dispositivo que no deba ser asignable, seleccione No Users.

- **Para hacer que el dispositivo sea asignable, pero que no requiera autorización, haga clic en All Users.**

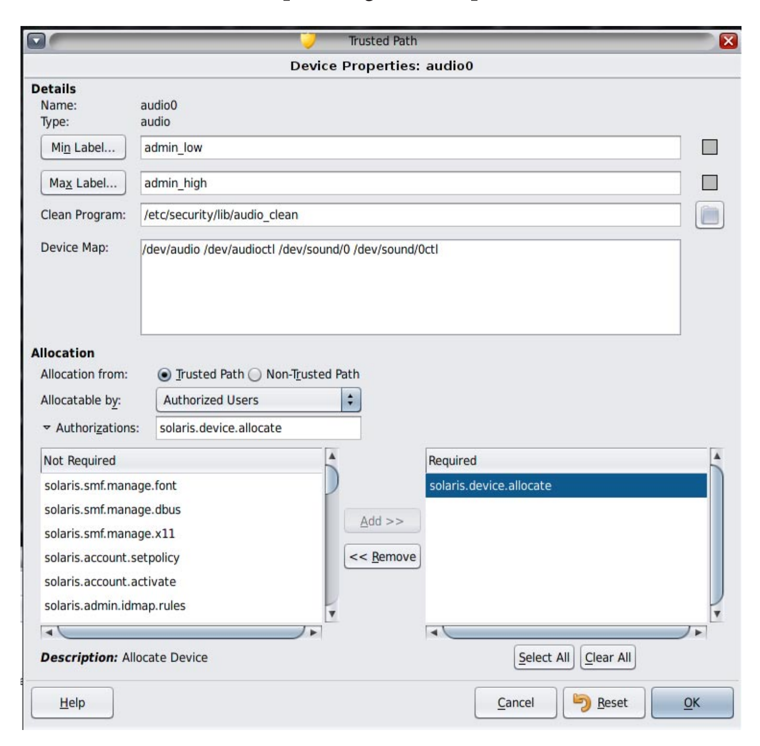
5 Especifique si el dispositivo se puede asignar de manera remota.

En la sección For Allocations From Non-Trusted Path, seleccione una opción de la lista Allocatable By. De manera predeterminada, la opción Same As Trusted Path está activada.

- **Para solicitar autorización del usuario, seleccione Allocatable by Authorized Users.**
- **Para hacer que los usuarios remotos no puedan asignar el dispositivo, seleccione No Users.**
- **Para hacer que cualquiera pueda asignar el dispositivo, seleccione All Users.**

6 **Si el dispositivo es asignable, *y* su sitio ha creado nuevas autorizaciones para dispositivos, seleccione la autorización adecuada.**

El cuadro de diálogo siguiente muestra que se requiere la autorización `solaris.device.allocate` para asignar el dispositivo `cdrom0`.



Para crear y utilizar autorizaciones para dispositivos específicas del sitio, consulte "Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)" en la página 257.

7 **Para guardar los cambios, haga clic en OK.**

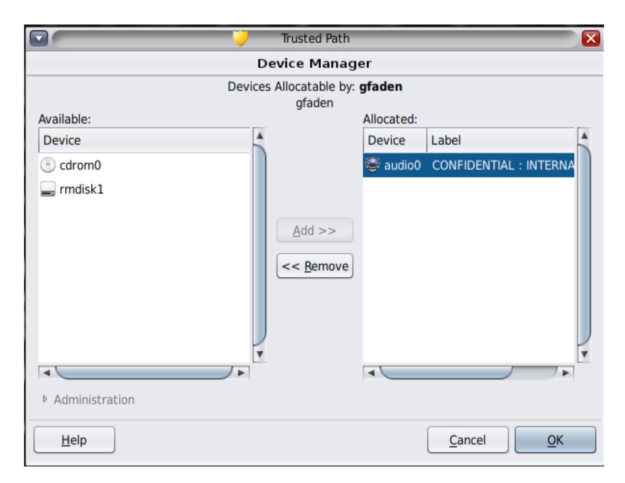
▼ Cómo revocar o reclamar un dispositivo en Trusted Extensions

Si un dispositivo no aparece en Device Allocation Manager, puede que ya se encuentre asignado o que esté en estado de error de asignación. El administrador del sistema puede recuperar el dispositivo para su uso.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global. Este rol cuenta con la autorización `solaris.device.revoke`.

1 **En el menú Trusted Path, seleccione Allocate Device.**

En la siguiente figura, el dispositivo de audio ya está asignado a un usuario.



2 **Haga clic en el botón Device Administration.**

3 **Compruebe el estado de un dispositivo.**

Seleccione el nombre del dispositivo y active el campo State.

- **Si el campo State dice Allocate Error State, haga clic en el botón Reclaim.**
- **Si el campo State dice Allocated, realice una de las siguientes acciones:**
  - **Solicite al usuario del campo Owner que desasigne el dispositivo.**
  - **Para llevar a cabo la desasignación forzosa del dispositivo, haga clic en el botón Revoke.**

4 **Cierre Device Allocation Manager.**

▼ Cómo proteger los dispositivos no asignables en Trusted Extensions

La opción No Users de la sección Allocatable By del cuadro de diálogo Device Configuration con frecuencia se utiliza para el búfer de trama y la impresora, que no requieren asignación para su uso.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 **En el menú Trusted Path, seleccione Allocate Device.**

2 **En Device Allocation Manager, haga clic en el botón Device Administration.**

3 **Seleccione la impresora o el búfer de trama nuevos.**

a. **Para hacer que el dispositivo no sea asignable, haga clic en No Users.**

b. **(Opcional) Restrinja el rango de etiquetas en el dispositivo.**

i. **Establezca la etiqueta mínima.**

Haga clic en el botón Min Label... y seleccione una etiqueta mínima del generador de etiquetas. Para obtener información sobre el generador de etiquetas, consulte "Generador de etiquetas en Trusted Extensions" en la página 43.

ii. **Establezca la etiqueta máxima.**

Haga clic en el botón Max Label... y seleccione una etiqueta máxima del generador de etiquetas.

Ejemplo 17–1 Impedir la asignación remota del dispositivo de audio

La opción No Users de la sección Allocatable By impide que los usuarios remotos escuchen las conversaciones en un sistema remoto.

El administrador de la seguridad configura el dispositivo de audio en Device Allocation Manager de la siguiente manera:

```
Device Name: audio
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: solaris.device.allocate

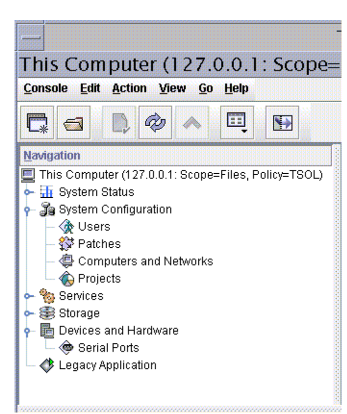
Device Name: audio
For Allocations From: Non-Trusted Pathh
Allocatable By: No Users
```

▼ Cómo configurar una línea de serie para el inicio de sesiones

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1 **Abra Solaris Management Console en el ámbito Files.**

FIGURA 17–1 Herramienta Serial Ports de Solaris Management Console



2 En Devices and Hardware, vaya a Serial Ports.

Escriba una contraseña cuando se le solicite. Siga la ayuda en pantalla para configurar el puerto de serie.

3 Para cambiar el rango de etiquetas predeterminado, abra Device Allocation Manager.

El rango de etiquetas predeterminado es de `ADMIN_LOW` a `ADMIN_HIGH`.

Ejemplo 17–2 Restricción del rango de etiquetas de un puerto de serie

Después de crear un dispositivo de inicio de sesión, el administrador de la seguridad restringe el rango de etiquetas del puerto de serie a una sola etiqueta: `Public`. El administrador define los siguientes valores en los cuadros de diálogo de Device Administration.

```
Device Name: /dev/term/[a|b]
Device Type: tty
Clean Program: /bin/true
Device Map: /dev/term/[a|b]
Minimum Label: Public
Maximum Label: Public
Allocatable By: No Users
```

▼ Cómo configurar un programa reproductor de audio para que se use en Trusted CDE

El siguiente procedimiento activa a un reproductor de audio para que se abra automáticamente en un espacio de trabajo de Trusted CDE cuando un usuario inserta un CD de música. Para obtener información sobre el procedimiento del usuario, consulte el ejemplo de “How to Allocate a Device in Trusted Extensions” de *Trusted Extensions User’s Guide*.

Nota – En el espacio de trabajo de Trusted JDS, los usuarios especifican el comportamiento de los medios extraíbles del mismo modo que lo especifican en un espacio de trabajo que no es de confianza.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1 **Edite el archivo `/etc/rmmount.conf`.**

Utilice el editor de confianza. Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

2 **Agregue el programa reproductor de CD del sitio a la acción `cdrom` en el archivo.**

```
action media action_program.so path-to-program
```

Ejemplo 17–3 Configuración de un programa reproductor de audio para su uso

En el siguiente ejemplo, el administrador del sistema hace que el programa `workman` esté disponible para todos los usuarios de un sistema. El programa `workman` es un programa reproductor de audio.

```
# /etc/rmmount.conf file
action cdrom action_workman.so /usr/local/bin/workman
```

▼ Cómo impedir la visualización de File Manager después de la asignación de un dispositivo

De manera predeterminada, File Manager aparece cuando se monta un dispositivo. Si no monta dispositivos que tengan sistemas de archivos, quizás desee impedir la visualización de File Manager.

Antes de empezar Debe estar con el rol de administrador del sistema en la zona global.

1 **Edite el archivo `/etc/rmmount.conf`.**

Utilice el editor de confianza. Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

2 **Encuentre las siguientes acciones `filemgr`:**

```
action cdrom action_filemgr.so
action floppy action_filemgr.so
```

3 **Comente la acción adecuada.**

El siguiente ejemplo muestra las acciones `action_filemgr.so` comentadas para los dispositivos `cdrom` y `diskette`.

```
# action cdrom action_filemgr.so
# action floppy action_filemgr.so
```

Cuando un CDROM o disquete está asignado, File Manager no se visualiza.

▼ Cómo agregar una secuencia de comandos device_clean en Trusted Extensions

Si no se especifica ninguna secuencia de comandos `device_clean` cuando se crea un dispositivo, se usa la secuencia de comandos predeterminada `/bin/true`.

Antes de empezar Debe tener lista una secuencia de comandos que purgue todos los datos utilizables del dispositivo físico y que devuelva `0` para que el proceso se realice correctamente. Para los dispositivos con medios extraíbles, la secuencia de comandos intenta expulsar el medio si el usuario no lo hace. La secuencia de comandos coloca el dispositivo en estado de error de asignación si el medio no se expulsa. Para obtener detalles sobre los requisitos, consulte la página del comando man `device_clean(5)`.

Debe estar con el rol de usuario `root` en la zona global.

1 **Copie la secuencia de comandos en el directorio `/etc/security/lib`.**

2 **En el cuadro de diálogo Device Administration, especifique la ruta completa para acceder a la secuencia de comandos.**

a. **Abra Device Allocation Manager.**

b. **Haga clic en el botón Device Administration.**

c. **Seleccione el nombre del dispositivo y haga clic en el botón Configure.**

d. **En el campo Clean Program, escriba la ruta completa para acceder a la secuencia de comandos.**

3 **Guarde los cambios.**

Personalización de autorizaciones para dispositivos en Trusted Extensions (mapa de tareas)

En el siguiente mapa de tareas, se describen los procedimientos para cambiar las autorizaciones para dispositivos en el sitio.

Tarea	Descripción	Para obtener instrucciones
Crear nuevas autorizaciones para dispositivos.	Se crean autorizaciones específicas del sitio.	"Cómo crear nuevas autorizaciones para dispositivos" en la página 257
Agregar autorizaciones a un dispositivo.	Se agregan autorizaciones específicas del sitio a dispositivos seleccionados.	"Cómo agregar autorizaciones específicas del sitio a un dispositivo en Trusted Extensions" en la página 260
Asignar autorizaciones para dispositivos a usuarios y roles.	Permite que los usuarios y los roles usen las autorizaciones nuevas.	"Cómo asignar autorizaciones para dispositivos" en la página 261

▼ Cómo crear nuevas autorizaciones para dispositivos

Si un dispositivo no requiere una autorización, de manera predeterminada, todos los usuarios pueden utilizar el dispositivo. Si se requiere una autorización, solamente los usuarios autorizados pueden utilizar el dispositivo.

Para denegar el acceso total a un dispositivo asignable, consulte el Ejemplo 17–1.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

1. **Edite el archivo `auth_attr`.**

   Utilice el editor de confianza. Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.

2. **Cree un encabezado para las autorizaciones nuevas.**

   Utilice el nombre de dominio de Internet de la organización en orden inverso seguido de componentes arbitrarios adicionales opcionales, como el nombre de la compañía. Separe los componentes con puntos. Finalice los encabezados con un punto.

   domain-suffix`.`*domain-prefix*`.`*optional*`.:::`*Company* `Header::help=`*Company*`.html`

3 Agregue entradas de autorización nuevas.

Agregue las autorizaciones (una autorización por línea). Las líneas se dividen con fines de visualización. Se incluyen las autorizaciones `grant` que activan a los administradores para asignar las autorizaciones nuevas.

```
domain-suffix.domain-prefix.grant:::Grant All Company Authorizations::
help=CompanyGrant.html
domain-suffix.domain-prefix.grant.device:::Grant Company Device Authorizations::
help=CompanyGrantDevice.html
domain-suffix.domain-prefix.device.allocate.tape:::Allocate Tape Device::
help=CompanyTapeAllocate.html
domain-suffix.domain-prefix.device.allocate.floppy:::Allocate Floppy Device::
help=CompanyFloppyAllocate.html
```

4 Guarde el archivo y cierre el editor.

5 Si usa LDAP como servicio de nombres, actualice las entradas de `auth_attr` en el Oracle Directory Server Enterprise Edition (servidor de directorios).

Para obtener información, consulte la página del comando man `ldapaddent`(1M).

6 Agregue las autorizaciones nuevas a los perfiles de derechos adecuados. Luego, asigne los perfiles a los usuarios y los roles.

Utilice Solaris Management Console. Asuma el rol de administrador de la seguridad y siga el procedimiento de Oracle Solaris "How to Create or Change a Rights Profile" de *System Administration Guide: Security Services*.

7 Utilice la autorización para restringir el acceso a unidades de cintas y de disquetes.

Agregar las autorizaciones nuevas a la lista de autorizaciones requeridas en Device Allocation Manager. Para conocer el procedimiento, consulte "Cómo agregar autorizaciones específicas del sitio a un dispositivo en Trusted Extensions" en la página 260.

Ejemplo 17–4 Creación de autorizaciones para dispositivos específicas

Un administrador de la seguridad de NewCo necesita establecer autorizaciones para dispositivos específicas para la compañía.

En primer lugar, el administrador escribe los siguientes archivos de ayuda y los coloca en el directorio `/usr/lib/help/auths/locale/C`:

```
Newco.html
NewcoGrant.html
NewcoGrantDevice.html
NewcoTapeAllocate.html
NewcoFloppyAllocate.html
```

Luego, el administrador agrega un encabezado a todas las autorizaciones para `newco.com` en el archivo `auth_attr`.

```
# auth_attr file
com.newco.:::NewCo Header::help=Newco.html
```

A continuación, el administrador agrega entradas de autorización al archivo:

```
com.newco.grant:::Grant All NewCo Authorizations::
help=NewcoGrant.html
com.newco.grant.device:::Grant NewCo Device Authorizations::
help=NewcoGrantDevice.html
com.newco.device.allocate.tape:::Allocate Tape Device::
help=NewcoTapeAllocate.html
com.newco.device.allocate.floppy:::Allocate Floppy Device::
help=NewcoFloppyAllocate.html
```

Las líneas se dividen con fines de visualización.

Las entradas `auth_attr` crean las siguientes autorizaciones:

- Una autorización para conceder todas las autorizaciones de NewCo
- Una autorización para conceder las autorizaciones para dispositivos de NewCo
- Una autorización para asignar una unidad de cinta
- Una autorización para asignar una unidad de disquete

Ejemplo 17–5 Creación de autorizaciones Trusted Path y Non-Trusted Path

De manera predeterminada, la autorización Allocate Devices activa la asignación desde adentro y desde afuera de Trusted Path.

En el siguiente ejemplo, la política de seguridad del sitio requiere la restricción de la asignación de CD-ROM remota. El administrador de la seguridad crea la autorización `com.someco.device.cdrom.local`. Esta autorización corresponde a las unidades de CD-ROM que se asignan con Trusted Path. La autorización `com.someco.device.cdrom.remote` corresponde a los pocos usuarios que tienen permiso para asignar una unidad de CD-ROM fuera de Trusted Path.

El administrador de la seguridad crea los archivos de ayuda, agrega las autorizaciones a la base de datos `auth_attr`, agrega las autorizaciones para los dispositivos y, luego, aplica las autorizaciones en los perfiles de derechos. Los perfiles se asignan a los usuarios que tienen permiso para asignar dispositivos.

- A continuación, se muestran las entradas de base de datos `auth_attr`:

  ```
  com.someco.:::SomeCo Header::help=Someco.html
  com.someco.grant:::Grant All SomeCo Authorizations::
  help=SomecoGrant.html
  com.someco.grant.device:::Grant SomeCo Device Authorizations::
  help=SomecoGrantDevice.html
  com.someco.device.cdrom.local:::Allocate Local CD-ROM Device::
  help=SomecoCDAllocateLocal.html
  com.someco.device.cdrom.remote:::Allocate Remote CD-ROM Device::
  help=SomecoCDAllocateRemote.html
  ```
- A continuación, se muestra la asignación de Device Allocation Manager:

Trusted Path activa a los usuarios autorizados para que utilicen Device Allocation Manager al asignar la unidad de CD-ROM local.

```
Device Name: cdrom_0
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: com.someco.device.cdrom.local
```

Non-Trusted Path activa a los usuarios para que asignen un dispositivo de manera remota mediante el comando `allocate`.

```
Device Name: cdrom_0
For Allocations From: Non-Trusted Path
Allocatable By: Authorized Users
Authorizations: com.someco.device.cdrom.remote
```

- A continuación, se muestran las entradas de derechos de perfiles:

```
# Local Allocator profile
com.someco.device.cdrom.local

# Remote Allocator profile
com.someco.device.cdrom.remote
```

- A continuación, se muestran los perfiles de derechos de los usuarios autorizados:

```
# List of profiles for regular authorized user
Local Allocator Profile
...

# List of profiles for role or authorized user
Remote Allocator Profile
...
```

▼ Cómo agregar autorizaciones específicas del sitio a un dispositivo en Trusted Extensions

Antes de empezar Debe estar con el rol de administrador de la seguridad o con un rol que incluya la autorización Configure Device Attributes. Ya debe haber creado las autorizaciones específicas del sitio, como se describe en "Cómo crear nuevas autorizaciones para dispositivos" en la página 257.

1 Siga el procedimiento de "Cómo configurar un dispositivo en Trusted Extensions" en la página 247.

a. Seleccione un dispositivo que deba protegerse con las autorizaciones nuevas.

b. Haga clic en el botón Device Administration.

c. Haga clic en el botón Authorizations.

Las autorizaciones nuevas se muestran en la lista Not Required.

d. Agregue las autorizaciones nuevas a la lista de autorizaciones Required.

2 **Para guardar los cambios, haga clic en OK.**

▼ Cómo asignar autorizaciones para dispositivos

La autorización Allocate Device activa a los usuarios para que asignen un dispositivo. Las autorizaciones Allocate Device y Revoke or Reclaim Device son adecuadas para los roles administrativos.

Antes de empezar Debe estar con el rol de administrador de la seguridad en la zona global.

Si los perfiles existentes no son adecuados, el administrador de la seguridad puede crear un perfil nuevo. Para ver un ejemplo, consulte "Cómo crear perfiles de derechos para autorizaciones convenientes" en la página 96.

● **Asigne al usuario un perfil de derechos que cuente con la autorización Allocate Device.**

Si necesita asistencia, consulte la ayuda en pantalla. Para conocer el procedimiento paso a paso, consulte "How to Change the RBAC Properties of a User" de *System Administration Guide: Security Services*.

Los siguientes perfiles de derechos activan un rol para que asigne dispositivos:

- All Authorizations
- Device Management
- Media Backup
- Object Label Management
- Software Installation

Los siguientes perfiles de derechos activan un rol para que revoque o reclame dispositivos:

- All Authorizations
- Device Management

Los siguientes perfiles de derechos activan un rol para que cree o configure dispositivos:

- All Authorizations
- Device Security

Ejemplo 17–6 Asignación de nuevas autorizaciones para dispositivos

En este ejemplo, el administrador de la seguridad configura las nuevas autorizaciones para dispositivos del sistema y asigna el perfil de derechos con las autorizaciones nuevas a usuarios de confianza. El administrador de la seguridad realiza lo siguiente:

1. Crea nuevas autorizaciones para dispositivos, como se establece en "Cómo crear nuevas autorizaciones para dispositivos" en la página 257
2. En Device Allocation Manager, agrega las nuevas autorizaciones para dispositivos a las unidades de cintas y de disquetes
3. Coloca las autorizaciones nuevas en el perfil de derechos NewCo Allocation
4. Agrega el perfil de derechos NewCo Allocation a los perfiles de usuarios y roles que están autorizados para asignar unidades de cintas y de disquetes

Así, los usuarios y los roles autorizados pueden usar las unidades de cinta y de disquetes del sistema.



CAPÍTULO 18

Auditoría de Trusted Extensions (descripción general)

En este capítulo, se describen las adiciones a la auditoría que Trusted Extensions proporciona.

Trusted Extensions y la auditoría

En un sistema configurado con el software Trusted Extensions, la configuración y la administración de la auditoría son similares a las de la auditoría en un sistema Oracle Solaris. Sin embargo, existen algunas diferencias:

- El software Trusted Extensions agrega al sistema clases, eventos y tokens de auditoría, y opciones de política de auditoría.
- En el software de Trusted Extensions, la auditoría está activada de manera predeterminada.
- No se admite la auditoría por zona de Oracle Solaris. En Trusted Extensions, todas las zonas se auditan de manera idéntica.
- Trusted Extensions proporciona herramientas para administrar las características de auditoría de los usuarios y para editar archivos de auditoría.
- Se utilizan dos roles, el administrador del sistema y el administrador de la seguridad, para configurar y administrar la auditoría en Trusted Extensions.

  El administrador de la seguridad planifica qué se debe auditar y establece asignaciones evento-clase específicas del sitio. Como en el SO Oracle Solaris, el administrador del sistema planifica los requisitos de espacio en el disco para los archivos de auditoría, crea un servidor de administración de auditoría e instala archivos de configuración de auditoría.

Gestión de auditoría por roles en Trusted Extensions

La auditoría en Trusted Extensions requiere la misma planificación que en el SO Oracle Solaris. Para obtener detalles sobre la planificación, consulte el Capítulo 29, "Planning for Oracle Solaris Auditing" de *System Administration Guide: Security Services*.

Configuración de roles para administración de auditoría

En Trusted Extensions, dos roles son responsables de la auditoría. El rol de administrador del sistema configura los discos y la red de almacenamiento de auditoría. El rol de administrador de la seguridad decide qué se debe auditar y especifica la información de los archivos de configuración de auditoría. Como en el SO Oracle Solaris, se deben crear los roles del software. Los perfiles de derechos para estos dos roles están incluidos. El equipo de configuración inicial creó el rol de administrador de la seguridad durante la configuración inicial. Para obtener detalles, consulte "Create the Security Administrator Role in Trusted Extensions" de *Trusted Extensions Configuration Guide*.

Nota – El sistema registra únicamente los eventos relativos a la seguridad que establecen los archivos de configuración de auditoría (es decir, eventos preseleccionados). Por lo tanto, en cualquier revisión de auditoría que se realice luego, solamente se pueden incluir los eventos que se hayan registrado. A causa de un error de configuración, puede que no se detecten los intentos de infracción de la seguridad del sistema o que el administrador no logre detectar al usuario que intentó infringir la seguridad. Los administradores deben analizar las pistas de auditoría con regularidad para verificar que no haya infracciones de la seguridad.

Tareas de auditoría en Trusted Extensions

Los procedimientos para configurar y gestionar la auditoría en Trusted Extensions difieren levemente de los procedimientos de Oracle Solaris.

- Uno de los roles administrativos realiza la configuración de la auditoría en la zona global. Luego, el administrador del sistema copia archivos de auditoría personalizados específicos de la zona global a las zonas con etiquetas. Con este procedimiento, las acciones del usuario se auditan de manera idéntica en la zona global y en las zonas con etiquetas.

  Para obtener detalles, consulte "Tareas de auditoría del administrador de la seguridad" en la página 265 y "Tareas de auditoría del administrador del sistema" en la página 265
- Los administradores de Trusted Extensions utilizan un editor de confianza para editar los archivos de configuración de auditoría. En Trusted CDE, los administradores de Trusted Extensions utilizan acciones de CDE para invocar el editor de confianza. Para ver la lista de acciones, consulte "Acciones de Trusted CDE" en la página 35.

- Los administradores de Trusted Extensions utilizan Solaris Management Console para configurar usuarios específicos. En esta herramienta se pueden determinar las características de auditoría específicas del usuario. Se requiere especificar las características del usuario solamente cuando las características de auditoría del usuario difieren de las características de auditoría de los sistemas en que el usuario trabaja. Para ver una introducción a la herramienta, consulte "Herramientas de Solaris Management Console" en la página 38.

Tareas de auditoría del administrador de la seguridad

Las siguientes tareas conciernen a la seguridad y, por consiguiente, son responsabilidad del administrador de la seguridad. Siga las instrucciones de Oracle Solaris, pero utilice las herramientas administrativas de Trusted Extensions.

Tarea	Para obtener instrucciones de Oracle Solaris	Diferencias de Trusted Extensions
Configure los archivos de auditoría.	"Configuring Audit Files (Task Map)" de *System Administration Guide: Security Services*	Utilice el editor de confianza. Para obtener detalles, consulte "Cómo editar archivos administrativos en Trusted Extensions" en la página 57.
(Opcional) Cambie la política de auditoría predeterminada.	"How to Configure Audit Policy" de *System Administration Guide: Security Services*	Utilice el editor de confianza.
Desactive y vuelva a activar la auditoría.	"How to Disable the Audit Service" de *System Administration Guide: Security Services*	La auditoría está activada de manera predeterminada.
Gestione la auditoría.	"Oracle Solaris Auditing (Task Map)" de *System Administration Guide: Security Services*	Utilice el editor de confianza. Ignore las tareas de auditoría por zona.

Tareas de auditoría del administrador del sistema

Las siguientes tareas son responsabilidad del administrador del sistema. Siga las instrucciones de Oracle Solaris, pero utilice las herramientas administrativas de Trusted Extensions.

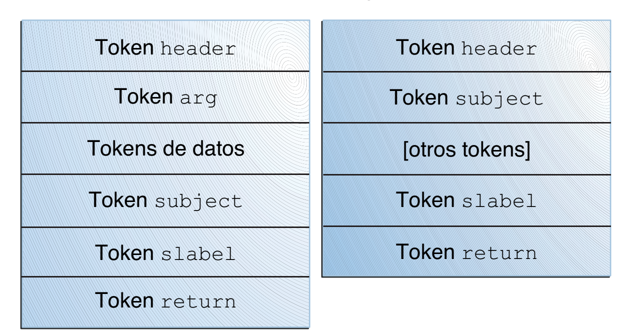
Tarea	Para obtener instrucciones de Oracle Solaris	Diferencias de Trusted Extensions
Cree un sistema de archivos ZFS dedicado a archivos de auditoría. Cree un alias `audit_warn`.	"Managing Audit Records" de *System Administration Guide: Security Services* "How to Configure the audit_warn Email Alias" de *System Administration Guide: Security Services*	Realice todas las tareas de administración en la zona global. Utilice el editor de confianza.

Tarea	Para obtener instrucciones de Oracle Solaris	Diferencias de Trusted Extensions
Copie o monte en bucle de retorno los archivos de auditoría personalizados en las zonas con etiquetas.	"Configuring the Audit Service in Zones (Tasks)" de *System Administration Guide: Security Services*	Monte en bucle de retorno o copie los archivos en cada zona con etiquetas una vez que se creen las zonas. Copie los archivos en la primera zona con etiquetas y, luego, copie la zona.
(Opcional) Distribuya los archivos de configuración de auditoría.	No hay instrucciones	Consulte "How to Copy Files From Portable Media in Trusted Extensions" de *Trusted Extensions Configuration Guide*
Gestione la auditoría.	"Oracle Solaris Auditing (Task Map)" de *System Administration Guide: Security Services*	Ignore las tareas de auditoría por zona.
Seleccione los registros de auditoría por etiqueta.	"How to Select Audit Events From the Audit Trail" de *System Administration Guide: Security Services*	Para seleccionar registros por etiqueta, utilice el comando `auditreduce` con la opción `-l`.

Referencia de auditoría de Trusted Extensions

El software de Trusted Extensions agrega al SO Oracle Solaris clases, eventos y tokens de auditoría, y también opciones de política de auditoría. Varios comandos de auditoría se amplían para manejar etiquetas. La siguiente figura muestra un registro de auditoría de núcleo y un registro de auditoría de nivel de usuario típicos de Trusted Extensions.

FIGURA 18–1 Estructuras típicas de registros de auditoría en un sistema con etiquetas



Clases de auditoría de Trusted Extensions

En la siguiente tabla, se enumeran en orden alfabético las clases de auditoría que el software de Trusted Extensions agrega al SO Oracle Solaris. Las clases se enumeran en el archivo

/etc/security/audit_class. Para obtener más información sobre las clases de auditoría, consulte la página del comando man audit_class(4).

TABLA 18–1 Clases de auditoría del servidor X

Nombre corto	Nombre largo	Máscara de auditoría
xc	X - Object create/destroy	0x00800000
xp	X - Privileged/administrative operations	0x00400000
xs	X - Operations that always silently fail, if bad	0x01000000
xx	X - All X events in the xc, xp, and xs classes (metaclass)	0x01c00000

Los eventos de auditoría del servidor X se asignan a estas clases según los criterios siguientes:

- **xc**: esta clase audita objetos de servidor de creación o destrucción. Por ejemplo, esta clase audita CreateWindow().
- **xp**: esta clase audita el uso de privilegios. El uso de privilegios puede ser correcto o incorrecto. Por ejemplo, ChangeWindowAttributes() se audita cuando un cliente intenta cambiar los atributos de una ventana de otro cliente. Esta clase también incluye rutinas administrativas, como SetAccessControl().
- **xs**: esta clase audita las rutinas que no devuelven mensajes de error X a los clientes en caso de errores causados por los atributos de seguridad. Por ejemplo, GetImage() no devuelve un error de BadWindow si no puede leer desde una ventana por falta de privilegios.

  Estos eventos se deben seleccionar para auditarlos únicamente cuando sean correctos. Si los eventos xs se seleccionan cuando son incorrectos, la pista de auditoría se llena de registros irrelevantes.
- **xx**: esta clase incluye todas las clases de auditoría X.

Eventos de auditoría de Trusted Extensions

El software Trusted Extensions agrega eventos de auditoría al sistema. Los eventos de auditoría nuevos y las clases de auditoría a las que los eventos pertenecen se enumeran en el archivo /etc/security/audit_event. Los números del evento de auditoría de Trusted Extensions se encuentran entre 9.000 y 10.000. Para obtener más información sobre los eventos de auditoría, consulte la página del comando man audit_event(4).

Tokens de auditoría de Trusted Extensions

En la siguiente tabla, se enumeran en orden alfabético los tokens de auditoría que el software de Trusted Extensions agrega al SO Oracle Solaris. Los tokens también se listan en la página del comando man audit.log(4).

TABLA 18–2 Tokens de auditoría de Trusted Extensions

Nombre de token	Descripción
"Token label" en la página 268	Etiqueta de sensibilidad
"Token xatom" en la página 269	Identificación de los átomos de las ventanas X
"Token xclient" en la página 269	Identificación de los clientes X
"Token xcolormap" en la página 270	Información sobre el color de las ventanas X
"Token xcursor" en la página 270	Información sobre los cursores de las ventanas X
"Token xfont" en la página 270	Información sobre las fuentes de las ventanas X
"Token xgc" en la página 271	Información sobre el contexto gráfico de las ventanas X
"Token xpixmap" en la página 271	Información sobre los mapas de píxeles de las ventanas X
"Token xproperty" en la página 271	Información sobre las propiedades de las ventanas X
"Token xselect" en la página 272	Información sobre los datos de las ventanas X
"Token xwindow" en la página 272	Información sobre las ventanas X

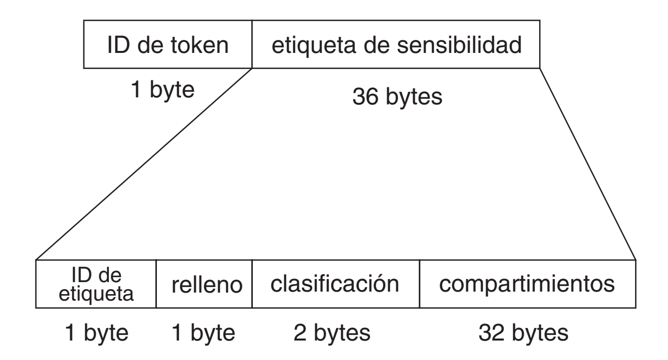
Token label

El token `label` contiene una etiqueta de sensibilidad. Este token contiene los siguientes campos:

- Un ID de token
- Una etiqueta de sensibilidad

La figura siguiente muestra el formato del token.

FIGURA 18–2 Formato del token label



Con el comando `praudit`, el token `label` se muestra de la siguiente manera:

```
sensitivity label,ADMIN_LOW
```

Token xatom

El token `xatom` contiene información relativa a un átomo X. Este token contiene los siguientes campos:

- Un ID de token
- La longitud de la cadena
- Una cadena de texto que identifica el átomo

Con `praudit`, el token `xatom` se muestra de la siguiente manera:

```
X atom,_DT_SAVE_MODE
```

Token xclient

El token `xclient` contiene información sobre el cliente X. Este token contiene los siguientes campos:

- Un ID de token
- El ID de cliente

Con `praudit`, el token `xclient` se muestra de la siguiente manera:

```
X client,15
```

Token xcolormap

El token `xcolormap` contiene información sobre los mapas de colores. Este token contiene los siguientes campos:

- Un ID de token
- El identificador del servidor X
- El ID de usuario del creador

La figura siguiente muestra el formato del token.

FIGURA 18–3 Formato para los tokens xcolormap, xcursor, xfont, xgc, xpixmap y xwindow

ID de token	XID	UID de creador
1 byte	4 bytes	4 bytes

Con `praudit`, el token `xcolormap` se muestra de la siguiente manera:

```
X color map,0x08c00005,srv
```

Token xcursor

El token `xcursor` contiene información sobre los cursores. Este token contiene los siguientes campos:

- Un ID de token
- El identificador del servidor X
- El ID de usuario del creador

La Figura 18–3 muestra el formato del token.

Con `praudit`, el token `xcursor` se muestra de la siguiente manera:

```
X cursor,0x0f400006,srv
```

Token xfont

El token `xfont` contiene información sobre las fuentes. Este token contiene los siguientes campos:

- Un ID de token
- El identificador del servidor X
- El ID de usuario del creador

La Figura 18–3 muestra el formato del token.

Con `praudit`, el token `xfont` se muestra de la siguiente manera:

```
X font,0x08c00001,srv
```

Token xgc

El token `xgc` contiene información sobre el xgc. Este token contiene los siguientes campos:

- Un ID de token
- El identificador del servidor X
- El ID de usuario del creador

La Figura 18–3 muestra el formato del token.

Con `praudit`, el token `xgc` se muestra de la siguiente manera:

```
Xgraphic context,0x002f2ca0,srv
```

Token xpixmap

El token `xpixmap` contiene información sobre las asignaciones de píxeles. Este token contiene los siguientes campos:

- Un ID de token
- El identificador del servidor X
- El ID de usuario del creador

La Figura 18–3 muestra el formato del token.

Con `praudit`, el token `xpixmap` se muestra de la siguiente manera:

```
X pixmap,0x08c00005,srv
```

Token xproperty

El token `xproperty` contiene información sobre varias propiedades de una ventana. Este token contiene los siguientes campos:

- Un ID de token
- El identificador del servidor X
- El ID de usuario del creador
- La longitud de la cadena
- Una cadena de texto que identifica el átomo

La figura siguiente muestra el formato del token `xproperty`.

FIGURA 18–4 Formato del token xproperty

ID de token	XID	UID de creador	strlen	cadena (nombre de átomo)
1 byte	4 bytes	4 bytes	2 bytes	N bytes

Con `praudit`, el token `xproperty` se muestra de la siguiente manera:

```
X property,0x000075d5,root,_MOTIF_DEFAULT_BINDINGS
```

Token xselect

El token `xselect` contiene los datos que se mueven entre las ventanas. Estos datos son una secuencia de bytes sin una estructura interna asumida ni una cadena de propiedades. Este token contiene los siguientes campos:

- Un ID de token
- La longitud de la cadena de propiedades
- La cadena de propiedades
- La longitud del tipo de propiedad
- La cadena del tipo de propiedad
- Un campo de longitud que da el número de bytes de los datos
- Una cadena de bytes que contiene los datos

La figura siguiente muestra el formato del token.

FIGURA 18–5 Formato del token xselect

ID de token	longitud de propiedad	cadena de propiedades	longitud de tipo de propiedad	tipo de propiedad	longitud de datos	datos de ventana
1 byte	2 bytes	N bytes	2 bytes	N bytes	2 bytes	N bytes

Con `praudit`, el token `xselect` se muestra de la siguiente manera:

```
X selection,entryfield,halogen
```

Token xwindow

El token `xwindow` contiene información sobre una ventana. Este token contiene los siguientes campos:

- Un ID de token
- El identificador del servidor X
- El ID de usuario del creador

La Figura 18–3 muestra el formato del token.

Con praudit, el token xwindow se muestra de la siguiente manera:

```
X window,0x07400001,srv
```

Opciones de política de auditoría de Trusted Extensions

Trusted Extensions agrega dos opciones de política de auditoría a las opciones de política de auditoría de Oracle Solaris existentes. Consulte la lista de políticas para conocer las nuevas opciones:

```
$ auditconfig -lspolicy
...
windata_down Include downgraded window information in audit records
windata_up   Include upgraded window information in audit records
...
```

Extensiones realizadas en comandos de auditoría de Trusted Extensions

Los comandos auditconfig, auditreduce y bsmrecord se extendieron a fin de manejar la información de Trusted Extensions:

- El comando auditconfig incluye las políticas de auditoría de Trusted Extensions. Para obtener detalles, consulte la página del comando man auditconfig(1M).
- El comando auditreduce proporciona la opción -l para filtrar registros por etiqueta. Para obtener detalles, consulte la página del comando man auditreduce(1M).
- El comando bsmrecord incluye los eventos de auditoría de Trusted Extensions. Para obtener detalles, consulte la página del comando man bsmrecord(1M).



Gestión de software en Trusted Extensions (tareas)

Este capítulo contiene información sobre cómo garantizar que el software de terceros se ejecute de manera confiable en un sistema que está configurado con Trusted Extensions.

Agregación de software a Trusted Extensions

Los programas de software que pueden agregarse a un sistema Oracle Solaris también pueden agregarse a un sistema que está configurado con Trusted Extensions. Además, es posible agregar los programas que utilizan las API de Trusted Extensions. La agregación de software en un sistema Trusted Extensions es similar a la agregación de software en un sistema Oracle Solaris que ejecuta zonas no globales.

Por ejemplo, los problemas de empaquetado afectan los sistemas que tienen zonas no globales. Los parámetros de los paquetes definen lo siguiente:

- **El ámbito de la zona del paquete**: el ámbito determina el tipo de zona en que puede instalarse un paquete específico.
- **La visibilidad del paquete**: la visibilidad determina si un paquete debe ser instalado e idéntico en todas las zonas.
- **La limitación del paquete**: una limitación es que un paquete deba instalarse en la zona actual únicamente.

En Trusted Extensions, los programas suelen instalarse en la zona global para que puedan utilizarlos los usuarios comunes en las zonas con etiquetas. Para obtener detalles sobre la instalación de paquetes en las zonas, consulte el Capítulo 25, "About Packages and Patches on an Oracle Solaris System With Zones Installed (Overview)" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*. También, consulte la página del comando man pkgadd(1M).

En un sitio de Trusted Extensions, el administrador del sistema trabaja junto con el administrador de la seguridad para instalar el software. El administrador de la seguridad evalúa si las adiciones de software cumplen la política de seguridad. Cuando el software requiere que los privilegios o las autorizaciones se efectúen correctamente, el rol de administrador de la seguridad asigna un perfil de derechos adecuado a los usuarios del software.

La importación de software desde medios extraíbles requiere autorización. Una cuenta con la autorización Allocate Device puede importar o exportar datos desde medios extraíbles. Los datos pueden incluir código ejecutable. Un usuario común sólo puede importar datos en una etiqueta dentro de la acreditación del usuario.

El rol de administrador del sistema es responsable de agregar los programas que apruebe el administrador de la seguridad.

Mecanismos de seguridad de Oracle Solaris para software

Trusted Extensions utiliza los mismos mecanismos de seguridad que el SO Oracle Solaris. Entre los mecanismos, se incluyen los siguientes:

- **Autorizaciones**: es posible que a los usuarios de un programa se les requiera una autorización específica. Para obtener información sobre las autorizaciones, consulte "Oracle Solaris RBAC Elements and Basic Concepts" de *System Administration Guide: Security Services*. También, consulte las páginas del comando man `auth_attr`(4) y `getauthattr`(3SECDB).
- **Privilegios**: se pueden asignar privilegios a los programas y a los procesos. Para obtener información sobre los privilegios, consulte el Capítulo 8, "Using Roles and Privileges (Overview)" de *System Administration Guide: Security Services*. También, consulte la página del comando man `privileges`(5).

  El comando `ppriv` proporciona una utilidad de depuración. Para obtener detalles, consulte la página del comando man `ppriv`(1). Para obtener instrucciones sobre el uso de esta utilidad con programas que funcionan en zonas no globales, consulte "Using the ppriv Utility" de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.
- **Perfiles de derechos**: los perfiles de derechos recopilan los atributos de seguridad en un solo lugar para asignarlos a los usuarios o a los roles. Para obtener información sobre los perfiles de derechos, consulte "RBAC Rights Profiles" de *System Administration Guide: Security Services*. Trusted Extensions agrega acciones de CDE para el tipo de ejecutables al que pueden asignarse los atributos de seguridad.
- **Bibliotecas de confianza**: las bibliotecas compartidas de manera dinámica que utilizan `setuid` y `setgid`, y los programas con privilegios pueden cargarse únicamente desde directorios de confianza. Como en el SO Oracle Solaris, se utiliza el comando `crle` para

agregar directorios de bibliotecas compartidas de un programa con privilegios a la lista de directorios de confianza. Para obtener detalles, consulte la página del comando man `crle(1)`.

Evaluación de software para la seguridad

Cuando se le asignan privilegios al software o cuando se lo ejecuta con un ID de grupo o de usuario alternativo, se convierte en un software *de confianza*. El software de confianza puede omitir aspectos de la política de seguridad de Trusted Extensions. Tenga en cuenta que puede convertir el software en confiable aunque podría no ser de confianza. El administrador de la seguridad debe esperar para otorgar privilegios al software hasta que se efectúe un examen minucioso que demuestre que el software utiliza los privilegios de manera confiable.

En un sistema de confianza, los programas se dividen en tres categorías:

- **Programas que no requieren atributos de seguridad**: algunos programas se ejecutan en un solo nivel y no requieren privilegios. Estos programas pueden instalarse en un directorio público, como `/usr/local`. Para obtener acceso, asigne el programa como comandos en los perfiles de derechos de los usuarios y de los roles.
- **Programas que se ejecutan como root**: algunos programas se ejecutan con `setuid 0`. Se puede asignar a estos programas un UID efectivo de `0` en un perfil de derechos. Luego, el administrador de la seguridad asigna el perfil a un rol administrativo.

  Consejo – Si la aplicación puede utilizar los privilegios de manera confiable, asigne los privilegios necesarios a la aplicación y no ejecute el programa como `root`.

- **Programas que requieren privilegios**: es posible que algunos programas requieran privilegios por motivos que no resultan evidentes. Incluso cuando un programa no ejerza ninguna función que pudiera infringir la política de seguridad del sistema, dicho programa podría realizar internamente una acción que infringe la seguridad. Por ejemplo, es posible que el programa utilice un archivo de registro compartido o que lea desde `/dev/kmem`. Para obtener información relativa a la seguridad, consulte la página del comando man `mem(7D)`.

  En algunas ocasiones, una invalidación de la política interna no es particularmente importante para el funcionamiento adecuado de la aplicación. En cambio, la invalidación proporciona una función conveniente para los usuarios.

  Si la organización tiene acceso al código de origen, compruebe si pueden eliminar las operaciones que requieran invalidaciones de la política, sin que se afecte el rendimiento de la aplicación.

Responsabilidades del desarrollador cuando se crean programas de confianza

Aunque el desarrollador de programas puede manipular los conjuntos de privilegios en el código de origen, si el administrador de la seguridad no asigna los privilegios necesarios al programa, el programa fallará. El desarrollador y el administrador de la seguridad deben cooperar cuando se crean programas de confianza.

El desarrollador que escribe un programa de confianza debe realizar lo siguiente:

1. Comprender cuándo el programa requiere privilegios para realizar su trabajo.
2. Conocer y aplicar las técnicas, como el escalonamiento de privilegios, para utilizar de un modo seguro los privilegios en los programas.
3. Tener en cuenta las consecuencias para la seguridad cuando asigna privilegios a un programa. El programa no debe infringir la política de seguridad.
4. Compilar el programa mediante las bibliotecas compartidas que están enlazadas al programa desde un directorio de confianza.

   Para obtener más información, consulte *Developer's Guide to Oracle Solaris 10 Security*. Para ver ejemplos de códigos para Trusted Extensions, consulte la *Trusted Extensions Developer's Guide* .

Responsabilidades del administrador de la seguridad para los programas de confianza

El administrador de la seguridad es el responsable de probar y evaluar el software nuevo. Después de establecer que el software es de confianza, el administrador de la seguridad configura los perfiles de derechos y otros atributos relevantes para la seguridad del programa.

Entre las responsabilidades del administrador de la seguridad, se incluyen las siguientes:

1. Asegurarse de que el programador y el proceso de distribución del programa sean de confianza.
2. A partir de una de las siguientes fuentes, determinar qué privilegios requiere el programa:
   - Preguntar al programador.
   - Buscar en el código de origen los privilegios que el programa prevé utilizar.
   - Buscar en el código de origen las autorizaciones que el programa requiere de los usuarios.
   - Usar las opciones de depuración para el comando `ppriv` a fin de buscar la utilización del privilegio. Para ver ejemplos, consulte la página del comando man `ppriv(1)`.
3. Examinar el código de origen para asegurarse de que se comporte de manera confiable con relación a los privilegios que el programa necesita para operar.

Si el programa no puede utilizar los privilegios de manera confiable, y usted puede modificar el código de origen del programa, modifique el código. Un consultor de seguridad o un desarrollador que tenga conocimientos sobre la seguridad puede modificar el código. Las modificaciones pueden incluir la separación de privilegios o la comprobación de autorizaciones.

La asignación de privilegios debe realizarse manualmente. Se pueden asignar privilegios a un programa que falla debido a la falta de privilegios. Como alternativa, el administrador de la seguridad puede decidir asignar un UID o un GID efectivo para que el privilegio resulte innecesario.

Procesos de confianza en el sistema de ventanas

En Solaris Trusted Extensions (CDE), los siguientes procesos del sistema de ventanas son de confianza:

- Panel frontal
- Subpaneles del panel frontal
- Menú Workspace
- File Manager
- Application Manager

Los procesos de confianza del sistema de ventanas están disponibles para todos, pero el acceso a las acciones administrativas está restringido a los roles en la zona global.

En File Manager, si una acción no se encuentra en uno de los perfiles de la cuenta, el icono de la acción no es visible. En el menú Workspace, si una acción no se encuentra en uno de los perfiles de la cuenta, la acción es visible, pero aparece un mensaje de error si se invoca la acción.

En Trusted CDE, el gestor de ventanas, `dtwm`, llama a la secuencia de comandos `Xtsolusersession`. Esta secuencia de comandos funciona con el gestor de ventanas para invocar las acciones que se iniciaron desde el sistema de ventanas. La secuencia de comandos `Xtsolusersession` comprueba los perfiles de derechos de la cuenta cuando la cuenta intenta iniciar una acción. En cualquiera de estos casos, si la acción se encuentra en un perfil de derechos asignado, la acción se ejecuta con los atributos de seguridad que están especificados en el perfil.

Adición de acciones de Trusted CDE

El proceso de creación y utilización de las acciones de CDE en Trusted Extensions es similar al proceso del SO Oracle Solaris. La agregación de las acciones se describe en el Capítulo 4, "Adding and Administering Applications" de *Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide*.

Como en el SO Oracle Solaris, el uso de las acciones puede controlarse con el mecanismo del perfil de derechos. En Trusted Extensions, se han asignado atributos de seguridad a varias acciones en los perfiles de derechos de los roles administrativos. El administrador de la seguridad también puede utilizar la herramienta Rights para asignar atributos de seguridad a las acciones nuevas.

En la siguiente tabla, se resumen las principales diferencias entre los sistemas Oracle Solaris y Trusted Extensions cuando se crean y se utilizan las acciones.

TABLA 19–1 Restricciones a las acciones de CDE en Trusted Extensions

Acciones de CDE de Oracle Solaris	Acciones de Trusted CDE
Cualquiera puede crear acciones nuevas en el directorio principal del originador. Una acción nueva puede ser utilizada automáticamente por su creador.	Una acción puede utilizarse únicamente si se encuentra en un perfil de derechos que está asignado al usuario. La ruta de búsqueda de acciones es diferente. Las acciones del directorio principal de un usuario se procesan en último lugar en vez de en primer lugar. Por lo tanto, nadie puede personalizar las acciones existentes. Los usuarios pueden crear una acción nueva en el directorio principal, pero es posible que la acción no pueda utilizarse. Los usuarios con el perfil de todos pueden utilizar una acción creada por ellos. De lo contrario, el administrador de la seguridad debe agregar el nombre de la acción nueva a uno de perfiles de derechos de la cuenta. Para iniciar la acción, el usuario utiliza File Manager. El administrador del sistema puede colocar acciones en directorios públicos.
Es posible arrastrar y soltar las acciones en el panel frontal.	El panel frontal es parte de la ruta de confianza. El gestor de ventanas reconoce solamente las acciones agregadas administrativamente que están ubicadas en los subdirectorios `/usr/dt` y `/etc/dt`. Incluso con el perfil de todos, un usuario no puede arrastrar una acción nueva al panel frontal. El gestor de ventanas no reconoce las acciones del directorio principal de un usuario. El gestor solamente comprueba los directorios públicos.
Las acciones pueden realizar operaciones con privilegios si las ejecuta el usuario `root`.	Las acciones pueden realizar las operaciones con privilegios si se les asignaron privilegios en un perfil de derechos que está asignado a un usuario.
Las acciones no se gestionan mediante la consola Solaris Management Console.	Las acciones se asignan a los perfiles de derechos en la herramienta Rights de la consola Solaris Management Console. Si se agregan acciones nuevas, el administrador de la seguridad puede hacer que estas acciones estén disponibles.

Gestión de software en Trusted Extensions (tareas)

La gestión de software en Trusted Extensions es similar a la gestión de software en un sistema Oracle Solaris que tiene zonas no globales. Para obtener detalles sobre las zonas, consulte la Parte II, “Zones” de *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

Cómo agregar un paquete de software en Trusted Extensions

Antes de empezar Debe estar en un rol que pueda asignar un dispositivo.

1. **Comience desde el espacio de trabajo adecuado.**

   - **Para instalar un paquete de software en la zona global, permanezca en la zona global.**
   - **Para instalar un paquete de software en una zona con etiquetas, cree un espacio de trabajo en esa etiqueta.**

     Para obtener detalles, consulte "How to Change the Label of a Workspace" de *Trusted Extensions User's Guide*.

2. **Asigne la unidad de CD-ROM.**

   Para obtener detalles, consulte "How to Allocate a Device in Trusted Extensions" de *Trusted Extensions User's Guide*.

3. **Instale el software.**

   Para obtener detalles, consulte "Dónde encontrar tareas de gestión de software" de *Administración de Oracle Solaris: administración básica*.

4. **Desasigne el dispositivo cuando haya terminado.**

   Para obtener detalles, consulte "How to Allocate a Device in Trusted Extensions" de *Trusted Extensions User's Guide*.

Cómo instalar un archivo de almacenamiento Java en Trusted Extensions

Este procedimiento descarga un archivo de almacenamiento Java (JAR) en la zona global. Desde la zona global, el administrador puede hacer que esté disponible para los usuarios comunes.

Antes de empezar El administrador de la seguridad debe haber verificado que el origen del programa Java sea de confianza, que el método de entrega sea seguro y que el programa pueda ejecutarse de manera confiable.

Está en el rol de administrador del sistema en la zona global. En Trusted CDE, el perfil de derechos de instalación de software incluye la acción de abrir para el código Java.

1 Descargue el archivo JAR en el directorio `/tmp`.

Por ejemplo, si selecciona el programa de software desde `http://www.sunfreeware.com`, utilice las instrucciones tituladas "Solaris `pkg-get` tool" (herramienta pkg-get de Solaris) que aparecen en este sitio.

2 Abra File Manager y vaya al directorio `/tmp`.

3 Haga doble clic en el archivo descargado.

4 Para instalar el software, responda las preguntas en los cuadros de diálogo.

5 Lea el registro de instalación.

Ejemplo 19–1 Descarga de un archivo JAR en una etiqueta del usuario

Para limitar el riesgo de seguridad, el administrador del sistema descarga el software en una sola etiqueta dentro del rango de acreditación de un usuario común. Luego, el administrador de la seguridad prueba el archivo JAR en esa etiqueta. Cuando el software supera la prueba, el administrador de la seguridad reduce el nivel de la etiqueta a `ADMIN_LOW`. El administrador del sistema instala el software en un servidor NFS a fin de que esté disponible para todos los usuarios.

1. En primer lugar, el administrador del sistema crea un espacio de trabajo en una etiqueta del usuario.
2. En ese espacio de trabajo, descarga el archivo JAR.
3. En esa etiqueta, el administrador de la seguridad prueba el archivo.
4. Luego, el administrador de la seguridad cambia la etiqueta del archivo a `ADMIN_LOW`.
5. Por último, el administrador del sistema copia el archivo a un servidor NFS cuya etiqueta sea `ADMIN_LOW`.

APÉNDICE A

Referencia rápida a la administración de Trusted Extensions

Las interfaces de Trusted Extensions amplían el SO Oracle Solaris. En este apéndice, se proporciona una referencia rápida sobre las diferencias. Para obtener una lista detallada de las interfaces, incluidas las rutinas de biblioteca y las llamadas del sistema, consulte el Apéndice B, "Lista de las páginas del comando man de Trusted Extensions".

Interfaces administrativas en Trusted Extensions

Trusted Extensions proporciona interfaces para el software. Las siguientes interfaces están disponibles únicamente cuando se ejecuta el software Trusted Extensions:

Secuencia de comandos `txzonemgr`	Proporciona un asistente basado en menú para crear, instalar, inicializar e iniciar las zonas con etiquetas. El título del menú es Labeled Zone Manager. Esta secuencia de comandos también proporciona opciones de menú para las opciones de red y de servicios de nombres, o a fin de establecer la zona global como cliente de un servidor LDAP existente.
Acciones de Trusted CDE	En Trusted CDE, Workspace Menu –> Application Manager –> Trusted_Extensions contiene acciones de CDE que configuran los archivos, instalan e inician las zonas, y simplifican otras tareas de Trusted Extensions. Para obtener información sobre las tareas que realizan estas acciones, consulte "Acciones de Trusted CDE" en la página 35. La ayuda en pantalla de Trusted CDE también describe estas acciones.
Admin Editor	Este editor de confianza se utiliza para editar archivos del sistema. En Trusted CDE, Workspace Menu –> Application Manager –> Trusted_Extensions –> Admin Editor invoca el editor de administración. En

	Trusted JDS, se invoca el editor desde la línea de comandos. Debe proporcionar el archivo que se va a editar como argumento; por ejemplo: `/usr/dt/bin/trusted_edit` *filename*
Device Allocation Manager	En Trusted Extensions, se utiliza esta interfaz gráfica de usuario para administrar dispositivos. Los administradores utilizan el cuadro de diálogo Device Administration para configurar dispositivos. Los roles y los usuarios comunes utilizan Device Allocation Manager para asignar dispositivos. La interfaz gráfica de usuario está disponible desde el menú Trusted Path.
Generador de etiquetas	Se invoca esta aplicación cuando el usuario puede elegir una etiqueta o una acreditación. Esta aplicación también aparece cuando un rol asigna etiquetas o rangos de etiquetas a los dispositivos, las zonas, los usuarios o los roles.
Selection Manager	Se invoca esta aplicación cuando un usuario o un rol autorizados intentan aumentar o disminuir el nivel de la información.
Menú Trusted Path	Este menú gestiona las interacciones con la base de computación de confianza (TCB). Por ejemplo, este menú tiene la opción de menú Change Password. En Trusted CDE, puede acceder al menú Trusted Path desde el área de selección de espacios de trabajo. En Trusted JDS, para acceder al menú Trusted Path, debe hacer clic en el símbolo de confianza que se encuentra a la izquierda de la banda de confianza.
Comandos administrativos	Trusted Extensions proporciona comandos para obtener etiquetas y realizar otras tareas. Para ver una lista de los comandos, consulte “Herramientas de la línea de comandos en Trusted Extensions” en la página 44.

Interfaces de Oracle Solaris ampliadas por Trusted Extensions

Trusted Extensions amplía los archivos de configuración, los comandos y las interfaces gráficas de usuario existentes de Oracle Solaris.

Comandos administrativos	Trusted Extensions agrega opciones a comandos seleccionados de Oracle Solaris. Para ver una lista, consulte la Tabla 2–5
Archivos de configuración	Trusted Extensions agrega dos privilegios: `net_mac_aware` y `net_mlp`. Para obtener información sobre el uso de `net_mac_aware`, consulte "Acceso a los directorios montados de NFS en Trusted Extensions" en la página 148. Trusted Extensions agrega autorizaciones a la base de datos `auth_attr`. Trusted Extensions agrega archivos ejecutables, incluidas las acciones de CDE, a la base de datos `exec_attr`. Trusted Extensions modifica los perfiles de derechos existentes en la base de datos `prof_attr`. También agrega perfiles a la base de datos. Trusted Extensions agrega acciones de CDE a los archivos ejecutables que pueden tener privilegios en la base de datos `exec_attr`. Trusted Extensions agrega campos a la base de datos `policy.conf`. Para obtener información sobre los campos, consulte "Valores predeterminados del archivo `policy.conf` en Trusted Extensions" en la página 81. Trusted Extensions agrega tokens de auditoría, eventos de auditoría, clases de auditoría y opciones de política de auditoría. Para ver una lista, consulte la "Referencia de auditoría de Trusted Extensions" en la página 266.
Solaris Management Console	Trusted Extensions agrega la herramienta Security Templates al conjunto de herramientas Computers and Networks.

	Trusted Extensions agrega la herramienta Trusted Network Zones al conjunto de herramientas Computers and Networks. Trusted Extensions agrega la ficha Trusted Extensions Attributes a las herramientas Users y Administrative Roles.
Directorios compartidos desde las zonas	Trusted Extensions le permite compartir directorios desde las zonas con etiquetas. Los directorios se comparten en la etiqueta de la zona mediante la creación de un archivo `/etc/dfs/dfstab` desde la zona global.

Valores predeterminados de seguridad que brindan mayor protección en Trusted Extensions

Trusted Extensions establece valores predeterminados de seguridad que brindan mayor protección que el SO Oracle Solaris:

Auditoría	De manera predeterminada, la auditoría está activada. El administrador puede desactivar la auditoría. Sin embargo, la auditoría suele requerirse en sitios que instalan Trusted Extensions.
Dispositivos	De manera predeterminada, la asignación de dispositivos está activada. De manera predeterminada, la asignación de dispositivos requiere autorización. Por lo tanto, de manera predeterminada, los usuarios comunes no pueden utilizar los medios extraíbles. El administrador puede eliminar el requisito de autorización. Sin embargo, la asignación de dispositivos suele requerirse en sitios que instalan Trusted Extensions.
Impresión	Los usuarios comunes pueden imprimir únicamente en las impresoras que incluyen la etiqueta del usuario en el rango de etiquetas de la impresora. De manera predeterminada, el resultado de la impresión tiene las páginas de la carátula y del ubicador. Estas páginas, y las páginas del cuerpo, incluyen la etiqueta del trabajo de impresión. De manera predeterminada, los usuarios no pueden imprimir archivos PostScript.

Roles	Los roles están disponibles en el SO Oracle Solaris, pero su uso es opcional. En Trusted Extensions, los roles son necesarios para la correcta administración. En el SO Oracle Solaris, es posible establecer el usuario `root` como rol. En Trusted Extensions, se establece el usuario `root` como rol para auditar con mayor eficacia al superusuario.

Opciones limitadas en Trusted Extensions

Trusted Extensions reduce el rango de opciones de configuración de Oracle Solaris:

Escritorio	Trusted Extensions ofrece dos escritorios: Solaris Trusted Extensions (CDE) y Solaris Trusted Extensions (JDS). Trusted Extensions ofrece el escritorio Solaris Trusted Extensions (GNOME).
Servicio de nombres	Se admite el servicio de nombres de LDAP. Todas las zonas deben administrarse desde un solo servicio de nombres.
Zonas	La zona global es una zona administrativa. Solamente el usuario `root` o un rol pueden entrar en la zona global. Por lo tanto, las interfaces administrativas que están disponibles para los usuarios comunes de Oracle Solaris no están disponibles para los usuarios comunes de Trusted Extensions. Por ejemplo, en Trusted Extensions, los usuarios no pueden abrir la consola Solaris Management Console. Las zonas no globales son las zonas con etiquetas. Los usuarios trabajan en las zonas con etiquetas.



APÉNDICE B

Lista de las páginas del comando man de Trusted Extensions

Trusted Extensions es una configuración del SO Oracle Solaris. En este apéndice, se proporciona una breve descripción de las páginas del comando man de Oracle Solaris que incluyen información sobre Trusted Extensions.

Páginas del comando man de Trusted Extensions en orden alfabético

Las siguientes páginas del comando man describen el software de Trusted Extensions en un sistema Oracle Solaris. Estas páginas del comando man sólo son relevantes en un sistema que está configurado con Trusted Extensions.

Página del comando man de Oracle Solaris	Síntesis
add_allocatable(1M)	Agrega entradas a las bases de datos de asignación
atohexlabel(1M)	Convierte una etiqueta en lenguaje natural a su equivalente de texto interno
blcompare(3TSOL)	Compara etiquetas binarias
blminmax(3TSOL)	Determina el vínculo entre dos etiquetas
chk_encodings(1M)	Comprueba la sintaxis del archivo de codificaciones de etiqueta
dtappsession(1)	Inicia una sesión nueva de Application Manager
fgetlabel(2)	Obtiene la etiqueta del archivo
getlabel(1)	Muestra la etiqueta de los archivos
getlabel(2)	Obtiene la etiqueta de un archivo

getpathbylabel(3TSOL)	Obtiene el nombre de ruta de la zona
getplabel(3TSOL)	Obtiene la etiqueta de un proceso
getuserrange(3TSOL)	Obtiene el rango de etiquetas de un usuario.
getzoneidbylabel(3TSOL)	Obtiene el ID de zona de la etiqueta de la zona
getzonelabelbyid(3TSOL)	Obtiene la etiqueta de la zona del ID de zona.
getzonelabelbyname(3TSOL)	Obtiene la etiqueta de la zona del nombre de la zona
getzonepath(1)	Muestra la ruta root de la zona que corresponde a la etiqueta especificada
getzonerootbyid(3TSOL)	Obtiene el nombre de ruta root de la zona del ID de root de la zona
getzonerootbylabel(3TSOL)	Obtiene el nombre de ruta root de la zona a partir de la etiqueta de la zona.
getzonerootbyname(3TSOL)	Obtiene el nombre de ruta root de la zona del nombre de la zona
hextoalabel(1M)	Convierte una etiqueta de texto interno a su equivalente en lenguaje natural.
labelbuilder(3TSOL)	Crea una interfaz de usuario basada en Motif para crear de manera interactiva una etiqueta o acreditación válidas
labelclipping(3TSOL)	Convierte una etiqueta binaria y la recorta al ancho especificado.
label_encodings(4)	Describe el archivo de codificaciones de etiqueta
label_to_str(3TSOL)	Convierte las etiquetas a cadenas en lenguaje natural
labels(5)	Describe los atributos de etiqueta de Trusted Extensions
libtsnet(3LIB)	Es la biblioteca de red de Trusted Extensions
libtsol(3LIB)	Es la biblioteca de Trusted Extensions
m_label(3TSOL)	Asigna y libera recursos para una etiqueta nueva
pam_tsol_account(5)	Comprueba las limitaciones de cuenta que originan las etiquetas

`plabel`(1)	Obtiene la etiqueta de un proceso
`remove_allocatable`(1M)	Elimina las entradas de las bases de datos de asignación
`sel_config`(4)	Establece las reglas de selección para las operaciones de copiar, cortar y pegar, y arrastrar y soltar
`setflabel`(3TSOL)	Mueve un archivo a una zona con la etiqueta de sensibilidad correspondiente
`smtnrhdb`(1M)	Gestiona las entradas de la base de datos de redes de Trusted Extensions
`smtnrhtp`(1M)	Gestiona las entradas de la base de datos de la plantilla para las redes de Trusted Extensions
`smtnzonecfg`(1M)	Gestiona las entradas de la base de datos de configuración para las redes de Trusted Extensions en zonas no globales
`str_to_label`(3TSOL)	Analiza las cadenas en lenguaje natural para una etiqueta
`tnctl`(1M)	Configura los parámetros de red de Trusted Extensions
`tnd`(1M)	Es el daemon de la red de confianza
`tninfo`(1M)	Muestra la información y las estadísticas de red de Trusted Extensions en el nivel del núcleo
`trusted_extensions`(5)	Presenta Trusted Extensions.
`TrustedExtensionsPolicy`(4)	Es el archivo de configuración de la extensión del servidor X de Trusted Extensions.
`tsol_getrhtype`(3TSOL)	Obtiene el tipo de host de la información de red de Trusted Extensions
`updatehome`(1M)	Actualiza los archivos de enlace y la copia del directorio principal para la etiqueta actual
`XTSOLgetClientAttributes`(3XTSOL)	Obtiene los atributos de etiqueta de un cliente X
`XTSOLgetPropAttributes`(3XTSOL)	Obtiene los atributos de etiqueta de una propiedad de una ventana

`XTSOLgetPropLabel`(3XTSOL)	Obtiene la etiqueta de una propiedad de una ventana
`XTSOLgetPropUID`(3XTSOL)	Obtiene el UID de una propiedad de una ventana
`XTSOLgetResAttributes`(3XTSOL)	Obtiene todos los atributos de etiqueta de una ventana o un mapa de píxeles
`XTSOLgetResLabel`(3XTSOL)	Obtiene la etiqueta de una ventana, un mapa de píxeles o un mapa de colores
`XTSOLgetResUID`(3XTSOL)	Obtiene el UID de una ventana o un mapa de píxeles.
`XTSOLgetSSHeight`(3XTSOL)	Obtiene la altura de la banda de la pantalla
`XTSOLgetWorkstationOwner`(3XTSOL)	Obtiene la propiedad de la estación de trabajo
`XTSOLIsWindowTrusted`(3XTSOL)	Determina si un cliente de confianza creó la ventana
`XTSOLMakeTPWindow`(3XTSOL)	Convierte esta ventana en una ventana Trusted Path
`XTSOLsetPolyInstInfo`(3XTSOL)	Establece la información para la creación de varias instancias
`XTSOLsetPropLabel`(3XTSOL)	Establece la etiqueta de una propiedad de la ventana
`XTSOLsetPropUID`(3XTSOL)	Establece el UID de una propiedad de una ventana
`XTSOLsetResLabel`(3XTSOL)	Establece la etiqueta de una ventana o un mapa de píxeles
`XTSOLsetResUID`(3XTSOL)	Establece el UID de una ventana, un mapa de píxeles o un mapa de colores
`XTSOLsetSessionHI`(3XTSOL)	Establece la etiqueta de sensibilidad alta de sesión para el servidor de la ventana
`XTSOLsetSessionLO`(3XTSOL)	Establece la etiqueta de sensibilidad baja de sesión para el servidor de la ventana
`XTSOLsetSSHeight`(3XTSOL)	Establece la altura de la banda de la pantalla
`XTSOLsetWorkstationOwner`(3XTSOL)	Establece la propiedad de la estación de trabajo

Páginas del comando man de Oracle Solaris modificadas por Trusted Extensions

Trusted Extensions agrega información a las siguientes páginas del comando man de Oracle Solaris.

Página del comando man de Oracle Solaris	Modificación de Trusted Extensions
allocate(1)	Agrega opciones para admitir la asignación de un dispositivo en una zona y la limpieza del dispositivo en un entorno de ventanas
auditconfig(1M)	Agrega la política de ventanas para la información con etiquetas
audit_class(4)	Agrega las clases de auditoría del servidor X
audit_event(4)	Agrega eventos de auditoría
auditreduce(1M)	Agrega un selector de etiquetas
auth_attr(4)	Agrega autorizaciones de etiqueta
automount(1M)	Agrega la capacidad para montar y, en consecuencia, ver los directorios principales de nivel inferior
cancel(1)	Agrega restricciones de etiqueta a la capacidad de un usuario para cancelar un trabajo de impresión
deallocate(1)	Agrega opciones para admitir la desasignación de un dispositivo en una zona, la limpieza del dispositivo en un entorno de ventanas y la especificación del tipo de dispositivo que debe desasignarse
device_clean(5)	Se invoca en Trusted Extensions de manera predeterminada.
exec_attr(4)	Agrega acciones de CDE como un tipo de objeto de perfil
getpflags(2)	Reconoce los indicadores de proceso NET_MAC_AWARE y NET_MAC_AWARE_INHERIT.
getsockopt(3SOCKET)	Obtiene el estado del control de acceso obligatorio, SO_MAC_EXEMPT, del socket.

getsockopt(3XNET)	Obtiene el estado del control de acceso obligatorio, SO_MAC_EXEMPT, del socket.
ifconfig(1M)	Agrega la interfaz all-zones
is_system_labeled(3C)	Determina si el sistema está configurado con Trusted Extensions.
ldaplist(1)	Agrega las bases de datos de red de Trusted Extensions
list_devices(1)	Agrega atributos, como etiquetas, que estén asociados con un dispositivo
lp(1)	Agrega la opción -nolabels
lpadmin(1M)	Agrega restricciones de etiqueta a la capacidad del administrador para administrar la impresión
lpmove(1M)	Agrega restricciones de etiqueta a la capacidad del administrador para mover un trabajo de impresión
lpq(1B)	Agrega restricciones de etiqueta para la visualización de la información de la cola de impresión
lprm(1B)	Agrega restricciones de etiqueta a la capacidad del emisor para eliminar solicitudes de impresión
lpsched(1M)	Agrega restricciones de etiqueta a la capacidad del administrador para detener y reiniciar el servicio de impresión
lpstat(1)	Agrega restricciones de etiqueta para la visualización del estado del servicio de impresión
netstat(1M)	Agrega la opción -R para visualizar atributos de seguridad ampliados
privileges(5)	Agrega privilegios de Trusted Extensions como PRIV_FILE_DOWNGRADE_SL.
prof_attr(4)	Agrega perfiles de derechos, como el de gestión de etiquetas de objetos
route(1M)	Agrega la opción -secattr para agregar atributos de seguridad ampliados a una ruta

setpflags(2)	Establece el indicador por proceso NET_MAC_AWARE.
setsockopt(3SOCKET)	Establece la opción SO_MAC_EXEMPT.
setsockopt(3XNET)	Establece el control de acceso obligatorio, SO_MAC_EXEMPT, en el socket.
smexec(1M)	Agrega opciones para admitir el tipo de acción de CDE
smrole(1M)	Agrega opciones para admitir la etiqueta de un rol
smuser(1M)	Agrega opciones para admitir la etiqueta de un usuario y otros atributos de seguridad, como el tiempo de inactividad permitido
socket.h(3HEAD)	Admite la opción SO_MAC_EXEMPT para iguales sin etiquetas.
tar(1)	Agrega etiquetas de inclusión en los archivos tar y en los archivos de extracción en función de la etiqueta
tar.h(3HEAD)	Agrega los tipos de atributos que se utilizan en los archivos tar con etiquetas
ucred_getlabel(3C)	Agrega la obtención del valor de etiqueta en una credencial de usuario.
user_attr(4)	Agrega los atributos de seguridad del usuario que son específicos para Trusted Extensions

Índice

B

C

D

L

M

R

S

T

U

V

Z